THE INTEGRATION OF INFORMATION AND COMMUNICATIONS
TECHNOLOGY IN FULL SPECTRUM OPERATIONS:
A CASE STUDY OF CJTF-101 IN AFGHANISTAN

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

CHARLES D. SMITH, MAJOR, U.S. ARMY
B.A., Southeastern Louisiana University, Hammond, Louisiana, 1996

Fort Leavenworth, Kansas
2010

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 10-06-2010 | Master's Thesis | AUG 2009 – JUN 2010 |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| The Integration of Information and Communications Technology in Full Spectrum Operations: A Case Study of CJTF-101 in Afghanistan | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |

| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
|---|---|
| Smith, Charles D., Major | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORG REPORT NUMBER |
|---|---|
| U.S. Army Command and General Staff College<br>ATTN: ATZL-SWD-GD<br>Fort Leavenworth, KS 66027-2301 | |

| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
|---|---|
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for Public Release; Distribution is Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The integration of Information and Communications Technology (ICT) is essential in today's contemporary operating environment. ICT now serves as a cross-sector enabler for all elements of national power due to the nature of Full Spectrum Operations, U.S. Interagency involvement, and the expansion of globalization. Using Combined Joint Task Force-101 (CJTF-101) in Afghanistan (2008-2009) as a case study, the lack of ICT coordination and synchronization among national and international stakeholders was evident. CJTF-101's experience showed that effects of poor coordination on the operating environment were significant. This research suggests that the U.S. Interagency, to include Department of Defense (DoD), can benefit from increased integration of the ICT Sector. Efforts should be made to train deploying personnel on ICT capabilities and relationships, develop partnerships with industry, incorporate professional development organizations with educational institutions, and create multilateral relationships from the national strategic level down to the tactical level. Additionally, unified action and the use of collaborative civil/military lesson-learned processes can greatly improve current and future operations. The establishment and implementation of an organization tasked with the responsibility to synchronize ICT strategies at the strategic, operational, and tactical levels is the keystone concept for the integration of ICT into full spectrum operations.

**15. SUBJECT TERMS**
Information and Communications Technology (ICT); Afghanistan; CJTF-101

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | 19b. PHONE NUMBER *(include area code)* |
| (U) | (U) | (U) | (U) | 102 | |

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

ii

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Charles D. Smith

Thesis Title:     The Integration of Information and Communications Technology in Full
                  Spectrum Operations: A Case Study of CJTF-101 in Afghanistan

Approved by:

_____, Thesis Committee Chair
Michael J. Burke, M.A.

_____, Member
Richard E. Berkebile, M.S.

_____, Member
John M. Curatola, Ph.D.

Accepted this 11th day of June 2010 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

ABSTRACT

THE INTEGRATION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY IN FULL SPECTRUM OPERATIONS: A CASE STUDY OF CJTF-101 IN AFGHANISTAN by Major Charles D. Smith, 102 pages.

The integration of Information and Communications Technology (ICT) is essential in today's contemporary operating environment. ICT now serves as a cross-sector enabler for all elements of national power due to the nature of Full Spectrum Operations, U.S. Interagency involvement, and the expansion of globalization. Using Combined Joint Task Force-101 (CJTF-101) in Afghanistan (2008-2009) as a case study, the lack of ICT coordination and synchronization among national and international stakeholders was evident. CJTF-101's experience showed that effects of poor coordination on the operating environment were significant. This research suggests that the U.S. Interagency, to include Department of Defense (DoD), can benefit from increased integration of the ICT Sector. Efforts should be made to train deploying personnel on ICT capabilities and relationships, develop partnerships with industry, incorporate professional development organizations with educational institutions, and create multilateral relationships from the national strategic level down to the tactical level. Additionally, unified action and the use of collaborative civil/military lesson-learned processes can greatly improve current and future operations. The establishment and implementation of an organization tasked with the responsibility to synchronize ICT strategies at the strategic, operational, and tactical levels is the keystone concept for the integration of ICT into full spectrum operations.

ACKNOWLEDGMENTS

TABLE OF CONTENTS

## ACRONYMS

ACCE        Afghanistan Communications Coordination Element

AFCEA       Armed Forces Communications and Electronics Association

ANDS        Afghanistan National Development Strategy

ASD/NII     Assistant Secretary of Defense / Network Information Integration

C4          Command, Control, Communications, and Computer Systems

CIO         Chief Information Officer

COIN        Counterinsurgency

DIME        Diplomatic, Information, Military, Economic

GAID        Global Alliance for ICT and Development

GIG         Global Information Grid

GIROA       Government of the Islamic Republic of Afghanistan

GNEC        Global Network Enterprise Construct

ICT         Information and Communications Technology (ies)

ISAF        International Security Assistance Force (Afghanistan)

ITU         International Telecommunications Union

MCIT        Ministry of Communications and Information Technology (Afghanistan)

MDG         Millennium Development Goals

NDU         National Defense University

STA         Senior Telecommunications Advisor

USAID       United States Agency for International Development

USFOR-A     United States Forces-Afghanistan

# ILLUSTRATIONS

TABLES

CHAPTER 1

INTRODUCTION


To enable Afghanistan to benefit further from Information and
Communication Technologies by becoming part of the global information society
while preserving Afghanistan's cultural heritage. To promote national goals as
well as in order to achieve a tolerant and vibrant Afghanistan, Afghanistan will
use Communications and ICTs to improve Government and social services
expeditiously and foster the rebuilding process, increase employment, create a
vibrant private sector, reduce poverty, and support underprivileged groups.
— Vision Statement of Afghan MCIT


Introduction

The study of how Afghanistan improved during 2008-2009 presented an

opportunity to identify the approach used to improve the Afghan government and the

lives of the Afghan people. By identifying the successes and failures of military-led

coordination efforts with the Afghan government in the communications sector, some

lessons may be identified that can improve future coordination efforts. Through this

research, an endeavor was made to answer a few key questions using a case study

approach of Combined Joint Task Force -101 in Afghanistan. This case study focused on

the integration of communications technology during full spectrum operations.


A Tool for Transition to Stable Peace

As our world transforms, we grow closer together as a civilization. Among the

myriad of changes in our global society, none has been more profound than the

proliferation of information and communications technology (ICT) systems. The

information revolution has changed our society into a connected, worldwide society of

societies. As technology evolved, connectivity began to define us. Individual national

1

economies are now interconnected in a global marketplace with free trade and transparency becoming more important to our global community. With this explosion of connectedness, a disparity exists in the speed of development that enables globalization. A significant part of the world remains unconnected and uninformed. As a global organization, the United Nations identified this problem and included progressive measures in their Millennium Development Goals (MDG).[1] In parts of the world where there remained a lack of ICT infrastructure, such as in Afghanistan prior to 2001, global problems erupted. Afghanistan represented a part of the global society that remained largely unconnected, uninformed, and unaware. With neighbors such as Pakistan, a nuclear-armed and globally connected nation, and Iran, Afghanistan became the "dark closet" where evil forces thrived. Thomas P.M. Barnett stated that "disconnected defines danger" and identified that Osama Bin Laden and Al Qaeda used these disconnected areas as safe havens to launch international acts of terrorism.[2] These disconnected cultures in Afghanistan presented a lucrative environment for such terrorists to organize, train, and equip their forces for battle, and they did.

As the US government plans and conducts operations globally in support of national and international interests, it is essential to identify the level of connectedness of the areas. Defining the endstate and exit strategies for the employment of any instruments of national power (Diplomatic, Information, Military, and Economic) begins at the initial planning stages and continues throughout the entire campaign. A critical strategic planning factor is to define the level of connectedness that exists in an area of interest. Planners must identify key infrastructure that enables governments to provide essential services to its people and to enable civil and military organizations to operate effectively.

This strategy must be developed, communicated, and supported at all levels with clearly defined roles and responsibilities. When the execution of our strategy requires the employment of an instrument of national power, it is essential that the strategies developed include an overarching concept for the utilization, and if required, the development of ICT to enable successful transition to civil authorities and promote global connectedness. Although, this integration and interdependence does not normally follow clear lines of command and control, such as a solely military operation, the nature of interagency coordination requires leaders at all levels to operate with other government agencies (OGAs), foreign governments (both friendly and hostile), Nongovernmental Organizations (NGOs), International Governmental Organizations (IGOs) and the private sector to achieve strategic objectives.[3]Additionally, when multiple instruments of national power are employed, this "unified action" (UA) requires effective information sharing procedures among all of the stakeholders.[4] The ability to integrate and synchronize actions between themselves and the other stakeholders is essential. Whether a deployed tactical, operational, or strategic ICT systems strategy is envisioned, the integration with, and eventual transition to the host nation's ICT infrastructure, is required to transfer responsibility back to the host nation following any intervention. This strategy must be conveyed to all stakeholders and enforced at the highest levels of government to achieve successful implementation. When this does not occur, as was the situation faced by Combined/Joint Task Force-101 (CJTF-101) in Afghanistan in 2008-2009, development efforts became inefficient and hindered to mission accomplishment.

Information and Communications Technologies

It is imperative to identify specific ICT terminologies, the composition of the ICT Sector, and how ICT enables cross-sector development. According to the World Bank, "Information and Communication Technologies (ICT) consists of the hardware, software, networks, and media used for the collection, storage, processing, transmission and presentation of information (voice, data, text, images), as well as related services."[5] For a clearer understanding, ICT is divided into two subcategories, infrastructure and technologies. Infrastructure, or Information and Communications Infrastructure (ICI), refers to physical telecommunications systems and networks (i.e., cellar, broadcast, cable, satellite, and postal) and the services that utilize them (i.e., Internet, voice, mail, radio, and television)."[6] Technologies, or Information Technologies (IT), "refer to the hardware and software used for information collection, storage, processing, and presentation."[7]

The continuous integration of information (data), communications technologies (systems), and the economies to support them creates the ICT Sector. Researchers at the National Defense University (NDU) report, "As a sector, ICT supports national capacity building . . ." and promotes the ". . . creation of powerful social and economic networks by dramatically improving communications and the exchange of information."[8]

ICT is a tool that connects individuals, communities, and societies to promote the sharing of information and coordination of resources, goods, and services beyond the confines of geographical and social boundaries. Governments, through the integrated and coordinated use of the ICT sector, can improve their responsiveness to their citizens by expanding reach and accessibility of services--and thereby enhancing government legitimacy and its ability to provide for its people.[9]

As a sector, a service, and a tool, ICT improves the overall wellbeing of our globally connected society. Developed nations are continuously improving their ICT capabilities, developing nations are acquiring and implementing ICT in support of their development, and underdeveloped nations do not know what they do not know. The United Nations identified that ICT is a tool for improving our global society. Many nations are following the UN MDGs and are developing their own ICT strategies. However, there remains many "seams" between connected and disconnected nations.[10] Our globalized society was significantly affected by a smart, agile, aggressive evil force that wreaked terror worldwide. It could happen again; and we must be prepared.

<div align="center">ICT in Full Spectrum Operations</div>

Changes in strategic considerations and the realization that this complex period requires a more protracted approach; a new level of integration of all of the instruments of national power was required. Collectively referred to as DIME (Diplomatic, Informational, Military, Economic), these instruments form the continuum of efforts for intervention in complex operations globally and leads to conclusion of operations on terms favorable to the US.[11] The Department of State (DoS) is the proponent for "D" or Diplomatic missions. The Department of Defense (DoD) is the proponent for "M" or Military application of DIME. The proponents for "I," Informational, and "E," Economic are more ambiguous and are supported by a multitude of agencies and departments. However, due to rapid globalization, the increased level of interaction made available by the information revolution and the improvements in ICT, a more integrated approach is required.

The President, as Commander in Chief, employs the Armed Forces of the US to achieve national strategic objectives.[12] The President and the Secretary of Defense, through the Chairman, Joint Chiefs of Staff, direct national efforts that provide Combatant Commanders with the national security policy and strategy. The Geographic Combatant Commander (GCC) is responsible for developing theater strategy in support of national strategic documents such as the *National Security Strategy*, *National Defense Strategy*, and the *National Military Strategy*. The GCC operates within a designated area of responsibility (AOR) and provides strategic direction for implementation of security cooperation programs throughout the assigned AOR. The GCC is also responsible for maintaining the theater strategic estimate and coordinating operations and strategies throughout the AOR in a developed Theater Security Cooperation Plan (TSCP). The TSCP, coupled with the strategic estimate, forms the basis of operations plans (OPLANs) that may be executed within the AOR. The TSCP contains criteria to determine when, where, and for what purpose major forces will be employed. The TSCP also considers "adjustments for multinational, interagency, IGO, OGA, and NGO circumstances . . ." and ". . . identification of termination criteria."[13]

DoD has identified offensive and defensive operations as decisive operations and considered other operations as supporting efforts. With our globalization and developments in ICT, this focus changed. As per DoD Directive 3000.05, Stability and Civil Support operations are now considered as equally important as offensive and defensive operations.[14]

Realizing that the operational environment changes, and based on the principles of unified action, the US Army developed its supporting concept that incorporated

offensive, defensive, and stability or civil support actions. The term *full spectrum operations* encompasses the full range of military action and a realization that each of these actions may occur simultaneously within the operating environment.[15]

A critical portion of the operational environment is the information environment. "The information environment is where humans and automated systems observe, orient, decide, and act upon information. . . ."[16] Information is defined as facts and data in any medium or form and "the meaning that a human assigns to data by means of the known conventions. . . ."[17] ICT, an element of the information environment, then exists and operates within the operational environment, subject to direct and indirect influence by internal and external factors. Identification of the capabilities, actors, and stakeholders within this environment is critical to develop an understanding of how to integrate ICT into operations.

<u>The Afghanistan Situation</u>

It is important to understand the operational environment the CJTF-101 CJ6 staff in Afghanistan experienced during their assignment in 2008-2009. Prior to deployment into Afghanistan, the 101st Airborne Division G6 (designated to become the CJTF-101 CJ6) searched for strategic and operational goals, objectives, and termination criteria in order to develop a coherent plan. However, none of the strategic or operational documents provided by the GCC, United States Central Command (USCENTCOM), or the previous headquarters, CJTF-82, contained the information required.[18] Upon arrival in the AOR in March 2008, CJTF-101 CJ6 staff met with Mr. James Baker, the Senior Telecom Advisor, Afghanistan Reconstruction Group, US Embassy. Baker provided an overview of the key players in the Ministry of Communications and Information

Technologies (MCIT), a brief outline of what the Afghanistan Reconstruction Group

(ARG) and the Senior Telecom Advisor (STA) were accomplishing at that time, and a

copy of the Defense and Technology Paper (DTP) number 45 produced by the National

Defense University (NDU).[19] This publication, labeled NDU's Defense and Technology

Paper #45, *Information and Communication Technologies for Reconstruction and*

*Development: Afghanistan Challenges and Opportunities*, by Larry Wentz, Frank

Kramer, and Stuart Starr, was the first document that provided information as to a

potential strategic and operational strategy for integration with MCIT and the ICT sector

overall. Baker laid out the details of very a chaotic environment with many stakeholders

and millions of dollars at stake. One key figure in the DTP represented a view of the

Afghanistan Infrastructure (see figure 1).



Figure 1.   Afghanistan's ICT Architecture
*Source*: Larry Wentz, Frank Kramer, and Stuart Starr, Technology Paper #45,
*Information and Communication Technologies for Reconstruction and Development:*
*Afghanistan Challenges and Opportunities* (Washington, DC: Center for Technology and
National Security Policy, National Defense University), 16.

Over the next several months, Baker and Mr. Robert Kinn, a contractor at the Office of the Assistant Secretary of Defense for Networks & Information Integration (OASD/NII) with several years experience working in Afghanistan, began laying out a plan for improving the interaction with the MCIT and other ICT Sector stakeholders. Kinn initiated weekly conference calls that included the CJTF-101 CJ6 staff and other ICT stakeholders to improve situational awareness in the ICT sector.

As later identified, Kinn possessed significant knowledge of MCIT, its officials, and the inter-workings of the ministry itself because he had worked Afghan ICT sector issues for the US government between the interagency in Afghanistan and Washington, DC going back to 2004. His experience included multiple assignments as Acting Senior Telecoms Advisor at the US Embassy, Kabul. Kinn's efforts to develop relationships between senior government officials in the MCIT, the International Security Assistance Force (ISAF), CJTF-101 staffs, the Interagency, and private sector investors were useful to the development of a working relationship with His Excellency (H.E.) Amir Zai Sangin, the Minister of MCIT for the Government of the Islamic Republic of Afghanistan (GIROA). Kinn created a series of meeting engagements that included representatives from the DoS, DoD, US Agency for International Development (USAID), and in coordination with NDU, the US Embassy in Kabul. Furthermore, this effort included many other organizations, both public and private, to coordinate efforts for reconstruction and development of the ICT sector and to synchronize ICT Sector development throughout the AOR. Quickly, the MCIT became the largest revenue-producing ministry of the GIROA.[20]

Unfortunately, in the fall of 2008, the US Embassy eliminated the ARG, including the STA position. With no centralized, authoritative individual or element to coordinate efforts or serve as a lead agent, it appeared that the DoS no longer considered the ICT Sector as important to overall reconstruction and stabilization efforts.

At the national strategic level, the ASD(NII)/DoD CIO, The Honorable John Grimes, and the US Joint Chiefs of Staff, J6, Vice Admiral Nancy Brown, met with H.E. Minister Sangin at his office in Kabul in August 2009. This meeting proved that some US national strategic interest remained in developing the ICT sector of Afghanistan. However, at the theater strategic and operational levels, the condition of Afghanistan ICT infrastructure and its capabilities were poorly understood. GIROA continually faced challenges of protecting, monitoring, and developing ICT both as a sector and as a service.
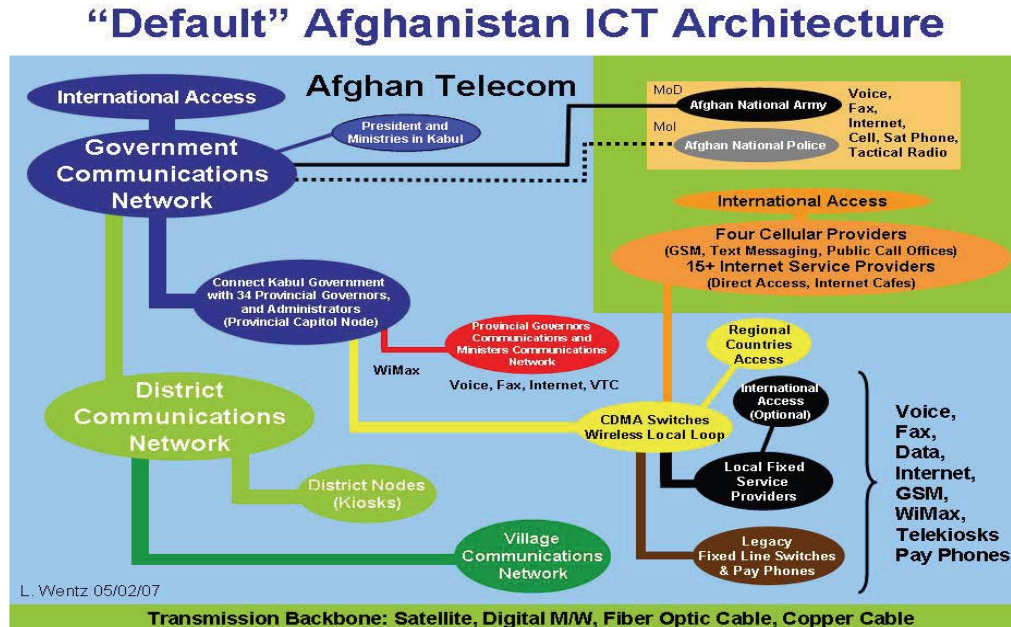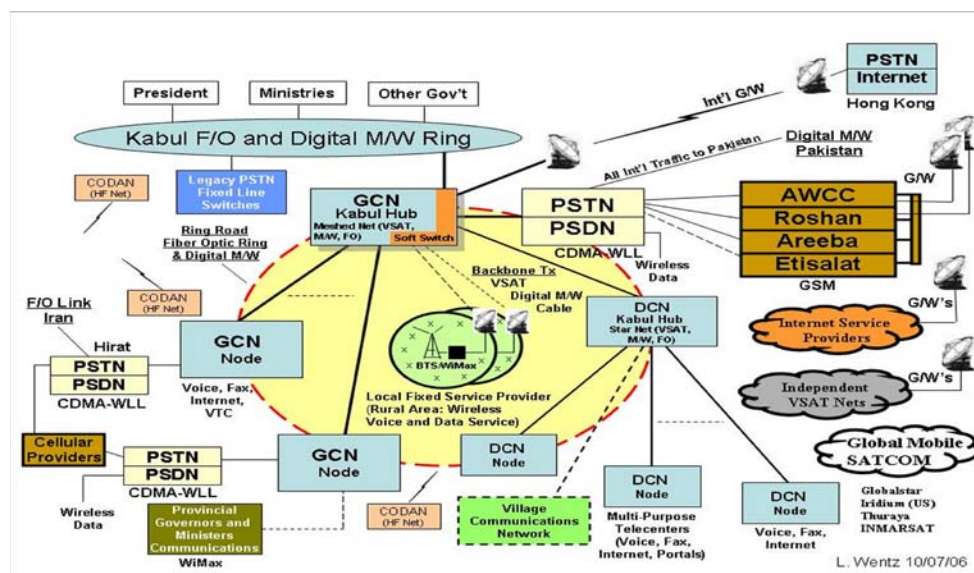


Figure 2.   Afghan ICT "As Is" Baseline

*Source*: Larry Wentz, Frank Kramer, and Stuart Starr, Technology Paper #45, *Information and Communication Technologies for Reconstruction and Development: Afghanistan Challenges and Opportunities* (Washington, DC: Center for Technology and National Security Policy, National Defense University), 20.

Although critical to developing the country, the maturity of the ICT sector was essential to its success and to the capability to transition communications services to commercial vendors. Commercial ICT infrastructure, critical to any transition of any future ICT services, was marginally being installed, operated, maintained, by very few private organizations and governed by MCIT.

The term "essential services" is defined as services that provide those things needed to sustain life.[21] However, the delivery of ICT and the amount of integration each service conducts in the ICT sector is critical. Current doctrine provides examples of services that meet the essential needs of people; availability of food, law enforcement, emergency services, water, electricity, shelter, health care, schools, transportation, and sanitation (trash and sewage).[22] The coordination and delivery of many of these identified services requires the use of communications systems. If the ICT sector is incapable of meeting the communications requirements, many of the service providers will bring their own systems into the operational area. This lack of coordination, especially with lengthy deployments or unorganized environments, can lead to the lack of interoperability among agencies. The lack of coordination can also lead to increased interference in an uncoordinated electromagnetic spectrum. ICT had been identified by researchers at NDU as both a "sector" and a "cross-sector enabler."[23] As a cross-sector enabler, ICT allows governments to improve their overall quality of their service and their responsiveness to their citizens. ICT provides the government a capability to coordinate better services for its citizens. The capability for a host nation government to coordinate and provide essential services to its citizens is increasingly important in this globally connected operational environment. Additionally, enabled governments that provide for the welfare

of its citizen's supports full spectrum operations doctrine. This ability is provided by a robust ICT sector, equipment, and trained individuals. The transition to a reliable host nation's communications infrastructure from communications systems that were initially deployed in the early stages of full spectrum operations can be complicated. This transition allows the redeployment or reassignment of communications providers and their equipment and establishes legitimacy of the host nation government. ICT is essential to the successful completion of full spectrum operations.

<div align="center">101st Airborne Division Assumes Duties as CJTF-101</div>

In June 2008, the 101st Airborne Division officially assumed the duties of the Combined Joint Task Force in Afghanistan from Combined/Joint Task Force 82 establishing the CJTF-101.[24] The official ceremony was on 4 June 2008 and the primary staff sections, particularly the G6 (communications staff), arrived as early as February 2008 to conduct relief in place operations with their respective staff counterparts. During this process, brief introductions were made to individuals who directly interfaced with the MCIT for the GIROA. One such introduction was to the STA, a DoS employee. The STA was employed in the ARG to act as the interface between the U.S. Embassy and the MCIT. At that time, Baker served as the STA.[25] Baker introduced the CJTF-101 CJ6 staff officers to Mr. Mohammad Ismail Bhat, Project Management Specialist for the MCIT and Chief Technical Officer (CTO) for Afghan Telecom, the government-owned communications company in Afghanistan. Mr. Bhat requested a meeting with CJTF-101 CJ6 personnel to present a brief overview of the projects underway at MCIT and a ". . . presentation on support to US Military in Afghanistan . . . issues and action plans to implement Optical Fiber Cable (OFC) solutions for International Security Assistance

Forces (ISAF), airbases and airports etc. to include a visit to communications hub."[26] The first meeting that CJTF-101 CJ6 personnel attended was in April 2008. This meeting was designed to help the new military officers understand the current operational environment with respect to ICT. Determining how to integrate ICT into the strategic and operational framework of civil/military operations proved extremely challenging. It was evident that no agency clearly understood the operational environment, how ICT was currently being employed, nor which organizations were stakeholders. The CJ6 could not establish a baseline understanding to begin coordination efforts. This lack of understanding greatly hindered the CJTF-101 CJ6's ability to conduct integrating planning or training.

According to the minutes of this first CJTF-101 CJ6-MCIT synchronization meeting, MCIT provided an overview of their ongoing projects and provided a tour of their network operations center.[27] In addition, several issues were addressed. First was the "attacks and turning –off of cell phone towers." This comment was likely based on reports that the Taliban was threatening telecom providers to turn off their towers after dark.[28] Reports such as BBC's "Taleban Threat Hits Afghan Phones" published on 12 March 2008, declared, "The Taleban threatened the companies, alleging that the networks were being used by Afghan and NATO troops to target them."[29] It was clear that this issue was a multinational issue and threatened all of the CJTF-101 lines of operation: Security, Governance, Development, and Information Activities (see Appendix A).[30] Oddly the MCIT personnel stated that "these actions will likely stop because the public have perceived that they are being hurt by these actions."[31] Another issue was the lack of coordination among GIROA Ministries. When questioned by the CJTF-101 CJ6 staff on how the ministries coordinate, MCIT officials were hesitant to comment.[32] However, an

issue arose in conversation about the Ministry of Interior (MOI) granting a three-digit-short code (100) to the Jalalabad's Nangahar Joint Provincial Coordination Center (JPCC) to which MCIT officials stated that they had no knowledge of such an agreement. Additionally, MCIT personnel stated that the Ministry of Interior was attempting to control the frequency spectrum and installing its own optical fiber cable for communications connectivity.[33] This combination of issues highlighted that a number of unrepresented stakeholders could benefit from a coordinated effort. This lack of coordination at the strategic and operational level, and between the US Interagency, ISAF elements and the CJTF-101 proved to be a significant issue that would not be solved in any quick or concise manner. The lack of a strategic vision, operational endstate, or tactical integration throughout the AOR highlighted the requirement for interaction and synchronization with commercial ICT providers, civil and military organizations, MCIT, the whole government of GIROA, and the Afghan people.

Summary

As the 101st Airborne Division assumed its role as the CJTF-101 in Afghanistan in 2008, the ICT sector in the country lacked coordination. None of the OPLANs or campaign plans contained information on the ICT infrastructure, the ICT sector, tasks to define and develop it, or indications on how to utilize it in productive ways in support of the national or international objectives. It seemed that leaders at the highest levels did not consider the ICT sector of any real importance, nor showed an understanding of how much commercialization of the ICT tactical infrastructure could benefit the overall operation. There was no designated lead agency (lack of unity of command) designated to identify, plan, coordinate, or interact with MCIT or other stakeholders in the ICT sector.

Many projects were not synchronized (lack of unity of effort) which led to duplication of effort and a waste of resources. The CJTF-101 CJ6 identified a significant lack of coordination among the ICT Sector stakeholders and the civil-military organizations operating within the AOR.

In order to draw conclusions and make recommendations to correct this issue, this thesis attempts to answer the question; how can ICT be integrated in Full Spectrum Operations. Additionally, this thesis attempts to answer the following secondary questions in order to clearly answer the primary research question: (1) Why was the CJTF-101 CJ6 (US Military) the lead planner and integrator of national ICT sector development in Afghanistan; (2) Should ICT be considered an essential service; (3) Why is ICT important to a host nation government and its society; and (4) Which US Government (USG) agency or department should be organized, trained, and equipped to coordinate ICT services in the executing of US national and international policy.

To develop a concept to answer these questions it was necessary to make some assumptions. First, Afghanistan had maintained its ICT capability as well as the electricity to power the equipment through the end of 2007. Next, elements of the society, particularly the education sector, had the human capital to operate and maintain ICT technology. The environmental conditions allowed the use of subterranean, terrestrial, atmospheric, and/or space-based communications technology. Additionally, the electromagnetic spectrum was not compromised. Finally, the cultural atmosphere allowed technology to be utilized.

Throughout this research, several additional key terms remained constant. These key terms are listed as follows:

Commercialization: tactical theater level communications element installing the initial communications infrastructure and transitioning that capability to a commercial provider.[34]

Cyberspace**:** the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[35]

Full Spectrum Operations: "Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action--lethal and nonlethal--proportional to the mission and informed by a thorough understanding of all variables of the operational environment."[36]

ICT Sector: "As a sector, ICT supports national capacity building and export market focus and plays a critical role in reestablishing basic economic linkages by relieving communication bottlenecks from financial, governmental, and cultural information flows."[37]

Interagency: "United States government agencies and departments, including the Department of Defense."[38]

Stability Operations: Stability operations are a subset of post-conflict operations. They are "an overarching term encompassing various military missions, tasks, and activities conducted outside of the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential

governmental services, emergency infrastructure reconstruction, and humanitarian

relief."[39] The DoS identifies these activities as "reconstruction and stabilization

operations."

Due to the sensitive nature of specific details of the ICT systems operated in

Afghanistan, some information remains classified. However, all of the information

obtained in this research was open-source, declassified through the appropriate

authorities, or unclassified. To develop a reference of deficiencies in specific systems

would only place those systems and those who rely on those systems at risk for

exploitation and are not necessary for the development of this thesis. Only logical

deductions based on unclassified information were used to draw conclusions or

inferences. Additionally, the technical details of ICT are constantly changing but useful

to address, to a small degree, to understand the concepts presented; however, only

relevant technical terms and schematics were presented to gain a fundamental

understanding of the technology and its capabilities. Unlike Afghanistan, it was not

useful to consider the relationship of ICT and Full Spectrum Operations in a nation or

society that does not have such technical, cultural, educational, or physical capabilities or

characteristics. Due to the time and nature of changing technology and the operational

environment, this research was limited to the time period immediately prior to the

deployment of 101st Airborne Division to Afghanistan (February 2008) until

immediately following its redeployment (May 2009).

This thesis consists of five chapters. Chapter 1 introduces the concepts of ICT,

Full Spectrum Operations, and stabilization, reconstruction and development. This

chapter also provided the background of the CJTF-101 CJ6. Additionally, it addresses the

CJ6's interaction with the GIROA's MCIT and the ICT Sector in Afghanistan. Key

questions are presented as well as the key terms defined, key assumptions identified, and

limitations provided. Chapter 2 reviews the literature available on this topic and provides

a framework to integrate these ideas in an attempt to answer the key questions of this

thesis. Chapter 3 identifies the research methodology of the study and describes why this

type of case study was selected. Chapter 4 provides the analysis of the information

collected. Chapter 5 provides possible answers to the key questions of this thesis and

recommendations for organizations to use to develop training requirements, the

designation of an element to coordinate the actions of disparate stakeholders in the ICT

Sector and an organizational structure to support these efforts.

---

[1]World Bank Group's Global ICT Department, *ICT and MDGs - A World Bank Group Perspective* (Washington, DC: World Bank Group's Global ICT Department, 2003), 7.

[2]Thomas P.M. Barnett, *The Pentagon's New Map: War and Peace in the Twenty-First Century* (New York, NY: G.P. Putnam's Sons, 2004), 49.

[3]Chairman, Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2006), II-9.

[4]Ibid., II-10.

[5]World Bank Group, *Information and Communication Technologies A World Bank Group Strategy* (Washington, DC: The International Bank for Reconstruction and Development/The World Bank, 2002), 3.

[6]Ibid.

[7]Ibid.

[8]Larry Wentz, Frank Kramer, and Stuart Starr, *Information and Communication Technologies for Reconstruction and Development: Afghanistan Challenges and Opportunities* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2008), 4.

[9]Ibid.

[10]Barnett, 188-189.

[11]Chairman, Joint Chiefs of Staff, JP 3-0, I-2.

[12]Ibid.

[13]Ibid., I-5.

[14]Department of Defense, DoD Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations* (Washington, DC: Government Printing Office, 2008), 2.

[15]Department of the Army, Field Manual (FM) 3-0*, Operations* (Washington, DC: Government Printing Office, 2008), viii.

[16]Chairman, Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2006), I-1.

[17]Chairman, Joint Chiefs of Staff, Joint Publication (JP) 1-02*, Department of Defense Dictionary of Military and Associated Terms*, As Amended Through 19 August 2009 (Washington, DC: Government Printing Office, 2009), 262.

[18]MAJ Charles D. Smith, Personal Experience, March 2008 to May 2009.

[19]Wentz, Kramer, and Starr.

[20]Minister Amir Zai Sangin, "Facts of the MCIT till the end of third Quarter of the calendar year 1386" (Briefing, GIROA Parliament, Kabul, Afghanistan, 28 February 2008).

[21]Chairman, Joint Chiefs of Staff, Joint Publication (JP) 3-24, C*ounterinsurgency Operations* (Washington, DC: Government Printing Office, 2009), II-7.

[22]Ibid.

[23]Wentz, Kramer, and Starr, 4.

[24]Department of the Army, Orders 06-0300, Deployment to Operation Enduring Freedom (29 February 2008).

[25]James R. Baker, Electronic correspondence with author, 1 April 2008.

[26]Mohammad Ismail Bhat, E-mail to author, 29 March 2008.

[27]Ministry of Communications and Information Technology, Monthly Synchronization Meeting, MCIT Headquarters, Kabul Afghanistan, April 2008.

[28]Ibid., 5.

[29]Sanjoy Maunder, "Taleban Threat Hits Afghan Phones," *BBC News*, http://news.bbc.co.uk/2/hi/south_asia/7291833.stm (accessed 27 January 2009).

[30]CJTF-101 Staff, "CJTF-101 Campaign Plan" (Briefing by CJTF-101 staff at Joint Planning Group session, 6 March 2008), 8.

[31]Ministry of Communications and Information Technology, Synchronization Meeting, 5.

[32]Ibid.

[33]Ibid.

[34]Department of the Army*,* Field Manuel Interim (FMI) 6-02.45, *Signal Support to Theater Operations* (Washington, DC: Government Printing Office, 2008), 2-17.

[35]Christopher J. Castelli, "Defense Department Adopts New Definition of Cyberspace," *Inside the Air Force*, http://integrator.hanscom.af.mil/2008/May/05292008/ 05292008-24.htm (accessed 20 March 2010).

[36]Department of the Army, FM 3-0, 3-1.

[37]World Bank Group's Global ICT Department, 7.

[38]Chairman, Joint Chiefs of Staff, JP 1-02, 273.

[39]Chairman, Joint Chiefs of Staff, JP 3-0, GL-29.

CHAPTER 2

REVIEW OF LITERATURE

Introduction

Information and Communications Technology (ICT) is a global sector and

utilized by all the nations on the planet. As global connectivity is now a part of our

society, the interconnectedness of the human race brings us all closer to a global state. In

order to organize this potentially chaotic environment, global policies and regulations

provide standards for interconnectivity and protection of a country's sovereign right to its

frequency spectrum. A detailed look at a portion of the literature that addresses how ICT

is utilized in a variety of contexts, such as military applications in full spectrum

operations, was completed by using multiple formats; books, periodicals, journals,

biographies, theses, unpublished papers, and electronic literature such as email briefings,

reports, web pages, and software programs. This literature review was organized in a

thematic approach addressing international, national, and local/individual aspects of ICT

employment. Those themes address ICT throughout the world as a global phenomenon,

common to all people in both developed and developing countries. In a national aspect,

each country approaches the ICT sector somewhat differently, but under a common

premise set forth by the international community. This approach allows individual

countries, through cooperation and adherence to these common premises, to join the

greater global community.

As the focus of this research is limited geographically to Afghanistan, its policies,

and procedures were reviewed. Other international actors contributed significantly to ICT

sector development in Afghanistan, such as the United States and other the countries that

comprise the ISAF. Additionally, countries that share Afghanistan's international borders, Pakistan, Tajikistan, Uzbekistan, Turkmenistan, Iran, and other regional actors such as India have significant influence on the ICT sector and Afghanistan's terrestrial connections to the world community. Documentation on how ICT is integrated into military operations provides connection to the civil-military interaction. Finally, the actual integration of ICT into full spectrum operations in Afghanistan, required coordination with other elements of the US Interagency, ISAF, and USFOR-A staff, and telecom companies from international investors to the wholly-government owned Afghan Telecom company and its interest. The summary ties all of these issues together into a common theme for consideration and recommendation for improvement.

## Source Review

### ICT Throughout the World

In September 2000, the United Nations (UN) adopted a declaration that established and published the MDGs. This declaration required nations to develop a new global partnership to achieve eight specified goals by 2015.[1] This document provides specific guidance to its subordinate organizations and staffs in order to coordinate with UN member nations. One of those goals, Goal 8, is to "develop a global partnership for development" and the International Telecommunications Union (ITU) received the task to measure the results of this implementation (target 18F of Goal 8).[2] The goal of this target is to provide a mechanism for governments to cooperate with the private sector, and make available the benefits of new technologies, especially information and communications technologies.[3] The document identifies indicators for the ITU to monitor and report progress to the UN.

In 2001, the UN established the United Nations ICT Task Force and designated the ITU as the lead international agency for the monitoring and development of ICT around the world. Due to the enormity of this task, the ITU collaborated with other UN agencies and began to address the development of the information society. This meeting was named the World Summit on the Information Society (WSIS) and presented a forum for emerging technologies.[4]

In 2007 the Global Alliance for ICT and Development (GAID), created by the UN as a secretariat in the Department of Economic and Social Affairs, published GAID Series 1 of the Foundations of the Global Alliance for ICT and Development.[5] In this publication, the GAID described the principles, structure, and modalities then reviewed the guiding documents for implementation of the MDGs. This GAID publication proposed a business plan for UN partner nations to follow in application of ICT sector development.

ICT in National Societies (Countries)

In the United States, the Federal Communications Commission (FCC) is an independent federal agency responsible directly to Congress to regulate interstate and international communications by radio, television, wire, satellite, and cable. The FCC Strategic Plan 2009-2014 provides the goals and objectives to accomplish its mission but does not specifically address the UNs MDGs. Do to the nature of the ICT sector in the United States, its relationship globally, and its interdependency on worldwide communications partnerships, it may be appropriate for the FCC to address the MDGs as a part of its national strategy. This seems to be an example of the lack of ICT Sector integration globally.

MCIT promotes its progress well, as can been seen in publications and brochures such as the one passed out during a meeting of the Ambassador's Representatives at the MCIT building in Kabul in April 2008. This brochure provides updates to each of the ICT development goals and presents MCIT and their initiatives in a very positive light.[6] Additionally, MCIT maintains a comprehensive website that provides information and press releases on projects and development goals published in the ICT Sector Strategy.[7]

Professional organizations such as Armed Forces Communications and Electronics Association (AFCEA) operate internationally, including a chapter in Afghanistan, and produce periodicals such as "Signal Magazine" that addresses the growth of the ICT market.[8] One online forum used for collaboration of multinational, US Interagency, and even transnational stakeholders is Harmonieweb (http://www.harmonieweb.org).[9] This website utilizes technology to improve information sharing.

Many private corporations such as GLOBECOM, MTN Areeba, Roshan, and other telecom companies invest heavily in developing nations such as Afghanistan. According to information from MCIT and CJTF-101 CJ6, these companies provide realistic investment opportunities for growing the ICT market, increasing profits of MCIT through fees and charges for licensing and frequency spectrum allocations, and services to the local villages and communities.[10]

ICT in Civil and Military Applications

In the United States, the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII), and the DoD Chief Information Officer (CIO) provide national oversight across DoD with policy guidance specifically for ICT. At the

National Defense University, researchers at the Center for Technology and National Security Policy (CTNSP) author and publish Defense and Technology Papers (DTPs) and conduct visits to countries such as Afghanistan and Iraq. Such papers as DTP #45, focuses on the challenges and opportunities for integrating ICT in Afghanistan.[11]

When the Department of State (DoS) published its 2009 Mission Strategic Plan for the US Mission to Afghanistan, it did not include any language for the development, measurement, or involvement with the ICT sector in Afghanistan or the region.[12] In fact, it did not mention MCIT within the document, which indicates that DoS did not consider MCIT or the ICT sector worthy of addressing.

The United States Institute of Peace, United States Army Peacekeeping, and Stability Operations Institute produced the *Guiding Principles for Stabilization and Reconstruction*, which provided a strategic framework that included the ICT Sector and identified several ways to integrate ICT into stabilization and reconstruction tasks.[13]

DoD maintains its own library of publications that contribute to the integration of full spectrum operations, roles, responsibilities, and the interdependencies of governmental, nongovernmental, and interagency organizations. Joint Publications and US Department of the Army Regulations and Field Manuals provide detail descriptions about the roles and responsibilities of Army units operating in unilateral, multilateral, and joint operations both in the US Homeland and abroad.

Many electronic correspondences (email) between CJTF-101 and ARG, NDU, and ASD/NII personnel provided an in-depth view of the problems, frustrations, and successes of integrating ICT in Afghanistan.[14] Trip reports by high-ranking individuals to

provide a critical look at the problems and challenges for the people on the ground

highlighted the lack of integration and unity of effort among the desperate stakeholders.[15]

Face-to-face meetings were extremely beneficial in providing insight for what

other agencies were doing to develop the ICT sector in the region. Supervisors at

ASD/NII branch of DoD extended invitations for this author to participate in discussions

and joint exercises related to development of the ICT sector in Afghanistan. This author

participated in teleconferences, email correspondence, and personal discussions with

ASD/NII personnel on numerous occasions.[16]

ICT in Afghanistan

The GIROA developed an Afghan National Development Strategy (ANDS),

which provided direction to government agencies and set milestones for

accomplishments, including measures of performance and indicators to be assessed.[17] The

MCIT developed and published the ICT Sector Strategy, which identified the overall

strategy for ICT development in the country, a strategic vision, sources of support, key

stakeholders, and provided a framework for implementation.[18] The Minister of

Communications, H.E. Sangin, briefed the Afghan national parliament on the progress of

MCIT and the ICT Sector in February 2008. During this presentation, H.E. Sangin

identified one future goal of MCIT which was to provide "Phone and Internet for 2000

villages, clearly aligned with the UN's MDG and assisting the ITU's in analyzing one if

its indicators for success."[19]

<u>Transition from Military to Commercial
Communications Systems</u>

At the COCOM level, as planners update Theater Security Cooperation Plans and identify changes in the ICT operational environment, theater communications planners must be aware of the potential effects these changes may have on operations in the AOR. At the beginning of the Joint Operational Planning Process, communication planners remain in contact with their counterparts within the theater of operation. During the Joint Intelligence Preparation of the Operational Environment (JIPOE), communications planners at all levels and in all agencies/departments must gather and share information that will provide the commander a detailed understanding how the ICT environment will limit his operations. Due to the integrated nature of ICT, all aspects of the DIME are affected by what ICT services and capabilities can be leveraged in the AOR. As the military is primarily the source of ICT services at the initial entry of an operation, plans must be developed early at the strategic level for the eventual transition of ICT services to the host nation infrastructure as quickly as possible. The design of the network interfaces, the types of equipment, and the protocols used must be developed before the first initial-entry circuit is installed. Failure to plan adequately for the commercialization of the operation could result in lengthy deployments for communications personnel and equipment, a multitude of additional costs to transition the network after it is established, and the capabilities of the commander to prosecute the operation limited.

In the case of CJTF-101 in Afghanistan, no theater baseline was established or available to operational planners. CENTCOM had not published Annex K (C4 Operations) to the campaign plans. There was no baseline in which to gage the capabilities of the ICT infrastructure in Afghanistan. Reports from the ITU were vague

and not detailed enough to provide any clarity. Reports from MCIT were often misleading or the information was not accurate. For example, the locations of GCN, PCN, and VCN communications equipment were in the form of spreadsheets with only city names for locations and the date they were initially installed.[20] MCIT did not maintain location or capability information on any of the equipment licensed to telecom companies in the country. No system was in place to enforce violations of spectrum licensing or registration. No capability existed to monitor, control, or enforce frequency interference from internal or external sources. Due to potential corruption within the government, ICT equipment remained embargoed at ports of entry until customs officials received hefty payments for import taxes.

In some cases, commercial vendors such as the privately owned Afghan Wireless Communications Company (AWCC) were contracted to provide microwave relay connections for remote FOBs and COBs. The majority of these links were redundant links in case the primary circuits failed. The reliability of these microwave links was unacceptable for normal communications throughput. AWCC suffered from a lack of trained technicians, technical planners, and the lack of freedom of movement. Security was a major concern for their technicians who refused to travel at night. Technicians only repaired failed circuits during daylight hours. On at least one occasion, the Taliban captured AWCC communications engineers, held them for ransom, possibly tortured them for assisting ISAF, and eventually released them as a warning to other highly skilled workers. In other instances, communications towers were destroyed because the company refused to turn off its services during the night, due to the belief that the targeting of the Taliban occurred at night. The Taliban took responsibility for this

destruction but as many were likely extortion of the infrastructure by local thieves. There seemed so many barriers to progress in Afghanistan that it was doubtful that commercialization efforts would truly be available in any near-term capacity.

Eventually success did come when the wholly owned Afghan Telecom announced it had completed its first fiber-optic link within the country. Almost simultaneously, Afghan Telecom announced international gateway links through Uzbekistan with hopes of establishing a link with Pakistan. Other national initiatives emerged such as instituting a national emergency response number (119) as established in Afghanistan National Numbering Plan. The Afghan Telecom Regulatory Authority began leading meetings of the Frequency Management Board (FMB), which addressed the coordination and use of spectrum assignments. Processes were emplaced to address international spectrum violations to the ITU for enforcement. The establishment of a single point of contact within MCIT created an atmosphere of legitimacy and regular meeting of a MCIT Synchronization Meeting had resumed. As of May 2009, MCIT met regularly with representatives from ISAF and US Militaries, US and Afghan governmental organizations, and private commercial organizations. Their goal; coordinate ICT sector development throughout the country.

Beginning a commercialization effort was blindly confusing. With differing reports on capabilities, limited availability of funding capability (required Title 22 Authority), and competing intentions between Combined Security Transition Command-Afghanistan (CSTC-A), who held Title 22 Authority, Commercial Providers, Afghan Governmental Officials, and the CJTF-101 CJ6 (who held Title 10 Authority), the progress was extremely slow. It was difficult to identify the organization that had the

29

responsibility and the capability to conduct ICT infrastructure assessment and development at the theater level. Because of the scope of operating nationally and across the AOR, this mission clearly fell to the CENTCOM staff. As the COCOM, the CENTCOM staff had more access to recourses, funding and contracting vehicles, and technical expertise to conduct theater-wide ICT integration. However, it may have been due to the focus on Iraq that caused the delays.

One element specifically designated to provide theater strategic communications integration was 335th Theater Signal Command (TSC). Based on the unit's mission statement, it seemed logical that theater infrastructure development was clearly their responsibility.[21] Historically, theater signal planners have leveraged the process to transition from military to commercial networks and infrastructure in order to free up valuable tactical signal assets through commercialization of network assets.[22]

Recent experience during Operation Desert Shield, Operation Desert Storm, Bosnia, and Kosovo, tactical communications capabilities must be used for initial entry into an operational area. Additionally, these operations provided examples where a tactical theater level communications element was responsible for installing the initial communications infrastructure and then transitioning that capability to a commercial provider. The signal command, in coordination with the JTF and JTF Army Force (ARFOR), should begin planning to transition the communications network to commercial means as soon as directed by the GCC. Transitioning a communications network to another provider, while ensuring interruption of services to the user is minimized, is a complicated and precise process. Coordination with tactical signal brigades and embedded tactical signal organizations is important in maintaining visibility

of the status of contractual negotiations and ensuring requirements are adequately identified and fed into the contract documents. Commercialization can be a long lead-time process and consequently must be a factor in the initial planning process, and whenever possible, should include pre-negotiated commercial contracts for services.

The critical capability for ICT is to enable commanders at all levels to achieve Battle Command, where they can Understand, Visualize, Describe, and Direct within their operational environment throughout the operations process.[23]

<div align="center">Summary</div>

As this review provides views from respective levels of government and civilian applications both globally, nationally, regionally, and locally, it serves to set the context for this research. Summarizing the information into a coherent theme, ICT is an element of the international community with applications and implications down to the individual. ICT sector development provides essential services and enables government, countries, and especially individuals to prosper in a globally connected world. The literature proves that ICT is being addressed globally and that steps are being taken to protect, expand, and profit by developments in the global ICT sector.

---

[1]International Telecommunications Union, "The UN Millennium Development Goals," http://www.itu.int/ITU-D/ict/mdg/ (accessed 30 January 2010).

[2]Ibid.

[3]Ibid.

[4]International Telecommunications Union, "World Summit on The Information Society Forum 2009," Brochure, May 2009.

[5]Global Alliance for ICT and Development (GAID), *Foundations of the Global Alliance for ICT and Development*, ed. Aliye P. Celik (New York: United Nations, 2007), 1-120.

[6]Ministry of Communications and Information Technology, "Summary of Achievements in the Year 1386," Brochure, April 2008.

[7]Ministry of Communications and Information Technology, "Islamic Republic of Afghanistan," http://www.mcit.gov.af (accessed 28 January 2009).

[8]Armed Forces Communications and Electronics Association (AFCEA), *Signal* (March 2010), 1-89.

[9]Harmonieweb, "Applications," http://www.harmoneweb.org (accessed 30 December 2009).

[10]Mohammad Ismail Bhat, E-mail to author, 1 April 2008.

[11]Wentz, Kramer, and Starr.

[12]Department of State, "FY 2009, Mission Strategic Plan, US Mission to Afghanistan" (30 May 2007), 1.

[13]United States Institute of Peace and the U.S. Army Peacekeeping and Stability Operations Institute, *Guiding Principles for Stabilization and Reconstruction* (Washington, DC: United States Institute of Peace, 2009).

[14]Charles D. Smith, electronic correspondence, provided by author.

[15]Frank Kramer, Stuart Starr, Larry Wentz, "Information Communications Technology Support to Reconstruction and Development: Some Observations from Afghanistan" (Twelfth International Command and Control Research and Technology Symposium (ICCRTS), Newport, Rhode Island, 19-21 June 2007).

[16]Mohammad Ismail Bhat, E-mail to author, 29 March 2008.

[17]Islamic Republic of Afghanistan, Afghanistan National Development Strategy Secretariat, "Islamic Republic of Afghanistan: Afghanistan National Development Strategy-1387–1391 (2008–2013) A Strategy for Security, Governance, Economic Growth & Poverty Reduction" (Kabul, Afghanistan, 2008).

[18]Ministry of Communications and Information Technology, "Islamic Republic of Afghanistan ICT Sector Strategy (Draft)," 22 November 2007.

[19]Minister Amir Zai Sangin, "Facts of the MCIT till the end of third Quarter of the calendar year 1386" (Briefing, GIROA Parliament, Kabul, Afghanistan, 28 February 2008), 12.

[20]Hanan Hashimi, Afghanistan Ministry of Communications and Information Technology, Excel Spreadsheet on locations of GCN nodes, E-mailed to author, 1 April 2008).

[21]335th TSC Website.

[22]Department of the Army,FMI 6-02.45, 2-17, 2-18.

[23]Department of the Army, FM 3-0, 5-3.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

Conducting research on this particular topic required a rather unique approach. A search of the relevant methodologies identified that a participative case study provided the most appropriate technique due to the author's participation in the majority of relevant events during the period studied. Although this type of study presented several biases, it remained the most appropriate.

Participant Observation Case Study as a Methodology

According to Dr. Danny Jorgensen, Associate Professor of Sociology with the Center for Interdisciplinary Studies in Culture and Society at the University of South Florida, St. Petersburg, the methodology of participant observation case study seeks to uncover, make accessible, and reveal the means (realities) people use to make sense out of their daily lives.[1] Even though Jorgensen states that this type of methodology is "especially appropriate for exploratory studies," this methodology was most appropriate for this thesis and did meet the basic requirements; "human interaction, occurring as a part of everyday life situations, understanding human decisions, and flexible, in-depth analysis."[2] For these reasons, the participant observation case study method was chosen for this research. This type of case study provides the necessary depth and breadth for this research topic and allows a detailed analysis to be completed in order to answer the research questions. Additionally, Dr. Robert K. Yin, noted researcher and Adjunct

Professor at American University's School of International Studies, states that the case study format attempts to answer the "how" and "why" research question.[3]

## The Overall Design

Why use a case study approach, particularly a participant observation case study? According to Dr. Jorgensen, a case study contributes uniquely to our knowledge of individual, organizational, social, and political phenomena and allows an investigation to retain the holistic and meaningful characteristics of real-life events.[4] Such studies address ". . . organizational processes . . . international relations and the maturation of industries," all of which are elements of the research questions for this thesis.[5]

Design components of the participant observation case study include the study's question, its propositions, units of analysis, logic linking the data to the propositions, and the criteria for interpreting the findings.[6] Each of these elements individually addresses aspects of this thesis within the context of the participant observation method. In this particular participant observed case study, the thesis author is that participant.

In order to identify comparable units of analysis, the following were considered: the number of meetings conducted between the ISAF/US Military and MCIT; the number of projects coordinated with MCIT; number of ICT projects sponsored by international stakeholders; and the comparative amount of revenue generated by ICT projects in Afghanistan. The period for this analysis includes January 2008 thru July 2009. The conversion rate of the US dollar is historically set to the period of the analysis and does not make any adjustment for current market rates.

To link the data, logically, the propositions are considered commonly shared among all stakeholders. No evidence of willful misleading reports or opinions was

discovered. No adjustments were made to the data in order to make it fit neatly into any one category. There are different opinions as to the accuracy of the data collected by the International Telecommunications Union. However, that data stands as a record for the information collected and reported by MCIT to international monitoring agencies during this period.[7]

The standard for interpreting the findings is measured in US dollars, the number of physical meetings, and the number of projects coordinated. Telephone conversations and email correspondence were not considered an appropriate measure for this thesis due to the routine nature of these communications. Further, no actionable decisions were attributed to either phone or email correspondence. Decisions were made at physical meetings with records or minutes of those meetings available for review. Physical presence at a meeting was considered appropriate as designated by the minutes provided by one of the participants, which often included photographs of the participants.[8]

<div align="center">The Strategy</div>

The strategies for answering thesis questions using the case study methodology are exploratory, descriptive, or explanatory; in some cases, all three strategies could be used.[9] Social science studies include experiments, surveys, archival analysis, histories, and case studies and for this particular research, the case study was chosen.[10] Experiments were not appropriate, archives were not fully accessible or accurate, and surveys were too time-consuming for the time constraints of this research. Each type of study seeks to answer questions in the most effective way. As identified by Dr. Yinn, the exploratory strategy asks the "what" and is favorable to the survey or archival strategy.[11] The descriptive strategy asks the "who and where . . . how many . . . how much . . ." and

is favorable to a survey or archival analysis.[12] While the explanatory strategy asks the "how and why". . . and is favorable to case studies, histories, and experiments.[13] This analysis is another reason the case study was chosen as the methodology for this research thesis.

## Sources of Evidence

The gathering of available documentation for this study followed prescribed guidelines for the collection and preservation of the chain of evidence. However, because many of the sources for this documentation are open-source, available on the internet, no certainty is made for the accuracy of that information. By using multiple sources, information could be verified as acceptable. The types of sources used for data collection included documentation, archival records, observation (participant), and physical artifacts.[14]

### Documentation

1. Letters, memorandums, email records.

2. Agendas and minutes of meetings.

3. Administrative documents and reports.

4. News clippings, websites, and other articles in mass media.

### Archival Records

1. Service records.

2. Organizational records (Historical reviews / After Action Reports).

3. Maps and charts (photos of maps and charts).

4. Lists of names and other relevant information.

5. Survey data such as collected by the ITU and World Bank.

6. Personal records such as notes, calendars, and telephone listings.

Interviews

Open-ended (informants).

Participant-Observation

This thesis author was the participant in this participant-observed case study and provided a unique perspective to the problem. One common problem in the participant observation study is "the ability to perceive reality from the viewpoint of someone 'inside' the case study rather than external to it."[15] This is certainly true of this thesis. The researcher attempted to identify biases at the beginning of this research in order to reduce the effects and to achieve an objective analysis of the data reviewed.

Physical Artifacts

A physical artifact is defined as a device, tool, or instrument, work of art, or some other physical evidence. In this research, the author acquired certain artifacts directly related to this study. Specifically, pieces of the original fiber optic cable installed in Afghanistan as well as marking tape identifying the Ministry of Communications in Afghanistan as the installer of such equipment were obtained by the author. The actual fiber optic cable utilized is commercial grade, shielded, multi-mode STM-III fiber optic cable.

Following the Principles of Data Collection

As it is important to maintain data integrity, there are rules for the collection and analysis of data used in case studies. These three principles are discussed here with an

explanation of their use in the context of research for this thesis. The three principles are using multiple sources of evidence, creating a case study database, and maintaining a chain of evidence.[16]

### Principle 1: Using Multiple Sources of Evidence.

Use of multiple sources in this case study "is the development of converging lines of inquiry, a process of triangulation . . . thus, any findings or conclusions in a case study is likely to be much more convincing and accurate if it is based on several different sources of information, following a corroboratory mode."[17] The data collected for this study was received from multiple sources and when additional information was available on the same meeting, engagement, project, etc., it was compared for accuracy. If there were any discrepancies, all were noted in order to maintain the validity of the data obtained. No data sources were combined into a common synthesis of ideas for clarity as that would have invalidated the integrity of the data obtained.

### Principle 2: Creating a Case Study Data Base.

The organization of data collection and the subsequent analysis by the researcher constitutes two separate collections of data. As a result of the increased ability to distribute documents electronically and the ability to conduct textual searches within documents, this thesis was compiled on multiple personal computer systems and provided to the Command and General Staff College (CGSC) for publication and distribution.

### Principle 3: Maintaining a Chain of Evidence.

Due to the open source availability of the information obtained in this study, no chain of custody was required. All information was gathered or provided by the

participant-observer, multiple informants, the internet, and through publically obtained

documents readily available to any other researcher.

<u>Interrelationships</u>

The purpose of this thesis is to research ways to integrate ICT into full spectrum

operations. Subsequent questions serve to define relevant concepts and to build a

construct to attempt to answer the primary question. First, as this research strategy was

based on a participate case study, it was important to establish the parameters for the

research, who the participant was, and why it was important to understand the situation

which the participant and the organization faced. In order to establish the period and

context it was important to discover the answer to the first question: Why was the CJTF-

101 CJ6 (US Military) the lead planner and integrator of national ICT sector development

in Afghanistan.

Based on the operational construct of the part of full spectrum operations

conducted in Afghanistan, COIN operations, one of the primary missions is to identify,

protect, and provide or ensure the provision of essential services. As the identification of

essential services typically indicates focus areas for commanders and staffs, it was

essential to determine the answer to the second question, should ICT be considered an

essential service. The answer to this question developed the basis to establish ICT as an

essential service under current military doctrine in direct support of full spectrum

operations.

As full spectrum operations has five clearly defined phases, it was important to

determine in which phase the integration of ICT would be most important. Conversely, it

was important to identify, if indeed, integration could not be isolated to one single phase,

and how the integration of ICT affects the endstate. To frame the case for ICT integration, it was important to answer a third question; why is ICT important to a host nation government and its society? The answer to this question helped to determine if ICT integration was indeed important to accomplish the endstate of full spectrum operations for both an intervening nation and a host-nation

Lastly, due to the integrated nature of ICT and its employment in throughout all elements of national power, one coordinator had to be identified. By answering the fourth question, which US Government (USG) agency or department should be organized, trained, and equipped to coordinate ICT services in the executing of US national and international policy, it was possible to identify a clear leader in the ICT integration in to full spectrum operations.

<p style="text-align:center;">Summary</p>

While validating the design of this case study, several criteria for analyzing the quality of the research design were used. Particularly, that validity and reliability must be addressed for the results to be useful. Four tests were applied to case study design; construct validity, internal validity, external validity, and reliability.[18] This thesis passed these tests for validity in that multiple sources were analyzed, pattern matching and explanation building were used, the results were reproducible based on the information analyzed, and this study could be used as a protocol for further studies in the ICT sector development field.[19] Further, the researcher acknowledged that the "design work actually continues beyond the initial design plans," which was evident in the broadening of the topic area from the original design.[20] Initially, the topic focused specifically on the identification of ICT as an "essential service" but a larger, more complex problem was

identified. This researcher reassessed the scope and broadened the topic to the current thesis design.

During the execution of this study, challenges were encountered in data collection and personal biases' of the observer. Data collection was difficult due to the limited amount of detailed information on the subject matter. References often referenced each other and obtaining archival records proved to be harder than planned. Additionally, the personal bias of the author as the participant in the case study limited the scope and depth of other aspects the research that could have been developed. The selection of a participant observed case study proved more reliable for gathering information that would not otherwise had been available. Personal interaction with many of the individuals, often used as case study informants, referenced in this research proved most reliable as a source of usable information.

The participant observed case study provided the necessary context to this research. This method was the most appropriate for this thesis topic and could be used again for the research of this subject.

---

[1]Dr. Danny L. Jorgensen, *Participant Observation, A Methodology for Human Studies* (Newbury Park, CA: SAGE Publications, Inc., 1989), 15.

[2]Ibid., 13.

[3]Dr. Robert K. Yin, *Case Study Research, Design and Methods* (Newbury Park, CA: SAGE Publications, Inc., 1989), 18.

[4]Jorgensen, 14.

[5]Ibid.

[6]Ibid., 29.

[7]International Telecommunications Union, "ICT Statistics Database," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx# (accessed 18 April 2010).

[8]Ministry of Communications and Information Technology, Synchronization Meeting, 1-4.

[9]Yin,15

[10]Ibid.

[11]Ibid., 18.

[12]Ibid.

[13]Ibid.

[14]Ibid., 85.

[15]Jorgensen, 93.

[16]Yin, 97.

[17]Ibid.

[18]Ibid., 41.

[19]Ibid.

[20]Ibid.

CHAPTER 4

ANALYSIS

Introduction

While conducting analysis of this topic, it became obvious there was no easy way

to integrate ICT into full spectrum operations. Initially it was evident that the term, full

spectrum operations, is an Army construct used to support DoD's Joint Operations

concept.[1] However, even the construct of joint operations does not sufficiently describe

the operational environment that CJTF-101 faced on its deployment to Afghanistan while

conducting Operation Enduring Freedom VIII. Multiple individuals and organizations

that represented the elements of national power were at work in the international,

combined, joint, full spectrum operations environment where NGOs, PVOs, private

industry, donor communities, and host-nation government interacted. The following

analysis attempts to answer the secondary research questions: (1) Why was CJTF-101

CJ6 (US Military) the lead planner and integrator of national ICT sector development in

Afghanistan; (2) Should ICT be considered an essential service; (3) Why is ICT

important to a host nation government and its society; (4) Which US Government agency

or department should be organized, trained, and equipped to coordinate ICT services in

the execution of US national and international policy? Finally, the concluding section

summarizes the answers to the secondary questions in order to present an argument to

answer the primary research question, how ICT can be integrated in full spectrum

operations.

Case Study Analysis

Interaction between the military and the Ministry of Communications and Information Technologies (MCIT) greatly improved during the 2008-2009 period. However, during the same period, the US Embassy dismantled the Afghan Reconstruction Group (ARG), including terminating the Senior Telecommunications Advisor (STA) position. Even with the increase in meetings between the military and MCIT, coordination as continuous as it had been with the STA in place. MCIT agreed to reestablish a synchronization meeting between military officials and MCIT officials.[2] Previously MCIT officials and members of CFC-A, including the STA, met weekly, and later monthly, in order to maintain situational awareness of the changes in country and to coordinate their respective activities. It is not known why these meetings ever stopped, but there clearly was a need for them, or some sort of coordination meeting to resume.

Coordination for ICT projects in Afghanistan varied greatly over the 15 months CJTF-101 was deployed in Afghanistan. Only three projects, the Afghan Optical Fiber Cable Network, the Governmental Communications Network (GCN), and the Provincial Governors Communications Network (PGCN) were recorded as being coordinated between MCIT and ISAF/US Military forces in 2007-2008. During the following year, multitudes of projects were coordinated with MCIT for research, analysis, or implementation. A number of these projects included extensions of the Afghan OFC project. Additional localized projects included the installation of a leased fiber optic cable network between Bagram and Kabul, de-confliction of antenna assets for "antenna hill" in Kabul, and multiple fiber installations within the city of Kabul. National projects included improvements in spectrum management, establishment of a National Emergency

45

Response Number (119), and the integration of Governor's Communications Network (GCN) for Voter Registration and National Election coordination. Other projects were addressed with MCIT for coordination, some were implemented, and some were not.

A key development index for ICT is the amount of subscribers that use the services offered. The UN recognized that the amount of ICT service was an excellent way to measure progress throughout the world. Accordingly, as developed in the Millennium Development Goals, the amount of subscribers provides a good indication of the economic, social, and infrastructure development in a country.

For the purpose of this analysis, both mobile (GSM/CDMA) and fixed line subscribers were combined into one data point. During this period, the population of Afghanistan realized a remarkable 127 percent increase in the number of ICT subscribers. This phenomenal improvement is likely due to significant enhancements in the ICT infrastructure and a commitment by MCIT to provide communications to underserved markets.

The amount of investment in the ICT sector of Afghanistan during this period was remarkable. Due to international investments, reinvestments of revenue, and donations from private donors, estimated investments totaled more than $1.2 billion. This investment was a 24 percent increase in the ICT market. With the increase of investments and numerous initiatives to improve access to ICT, the percentage of the population covered by ICT services increased. Between 2008 and 2009, the amount of the populations covered by the availability ICT improved from 70 percent to more than 80 percent of the population of Afghanistan.

Overall, the amount of ICT increase that occurred during this one-year period was remarkable. One major concern was the amount of information provided to, collected by, and reported by the ITU on Afghanistan. No central repository was available to correlate this information. However, one important development was the increase in investments to the coverage of the population. Even though the number of meetings between military representatives and MCIT officials, and the number of projects increased, there was no correlation that this increased interaction was responsible for the increases identified in other areas of the study.

Table 1.    Comparisons of Afghanistan ICT Data

|  | 2007 – 2008 | 2008-2009 |
|---|---|---|
| Number of Meetings Attended with MCIT | 3 | 16 |
| Number of Projects Coordinated with MCIT | 3 | 26 |
| Number of Subscribers (GSM, CDMA, Landline) | 5,400,000 | 12,242,899 |
| Amount of Investments (in US $ Millions) | US $1, 031 | US $1, 276 |
| Population Coverage (percentage of population) | 70% | 80% |

*Source*: Created by author.

CJTF-101 CJ6 as the Lead Planner
of National ICT in Afghanistan

In Afghanistan, during 2008-2009, significant changes occurred in the operational environment. One such change was that the STA position that provided a link between the MCIT and the US government was terminated. In late 2008, CJTF-101 CJ6 planners were developing plans for increased troop deployments and required a more detailed

understanding of the ICT sector affecting the AOR. Attempts to obtain information from MCIT did not produce the level of detail required. USFOR-A had not yet been established and there were no USCENTCOM personnel directly engaged in the ICT sector. Campaign plans did not address attempts for commercialization efforts or the transition of tactical communications to commercial, terrestrial communications systems. The capabilities of ICT infrastructure were unknown and there were no agencies or elements conducting assessments on its capability. During the same period, CJTF-101 CJ6 network engineers collaborated with commercial communications companies to extend communications links over terrestrial microwave line of sight communications towers throughout Afghanistan. As this endeavor became more viable, a need was realized that to enable the government of Afghanistan, greater coordination with MCIT was required.

The US military has a tendency to focus on mission accomplishment and endstate. That focus expanded to commercialization of communications and the redeployment and reassignment of tactical signal assets. Additionally, as noted by the Army Chief of Staff, the military is trained to plan, more so than any other agency.[3] As the largest US department present in Afghanistan, it seemed logical that DoD should play a significant role in coordinating actions with the host nation. During this period however, DoS removed their critical link into the MCIT, the STA of the ARG. Had this critical position remained filled, it may have had a significant impact on who would synchronize efforts with MCIT. Additionally, due to the lack of stability in ISAF HQ, and the fact that ISAF had contracted their communications capabilities to a commercial company, the CJTF-101 CJ6 was the only organization capable of conducting this mission. Since the CSTC-A

mission was to train and equip only the Afghan Security Forces, this mission did not include training or equipping government officials. USCENTCOM did assigned liaisons from 335th Theater Signal Command (TSC) to deploy forward to major locations around the country including Kabul, Bagram, and Kandahar, but due to reasons unknown, they did not interact with MCIT. Because the 335th TSC LNOs lacked the capability to conduct any real coordination with MCIT, they could not perform the coordination required between military forces and MCIT. It was obvious that the only organization capable of serving as the lead planner and integrator with MCIT was the CJTF-101 CJ6.

DoD had more resources than any other Interagency partner to do such coordination in Afghanistan. DoD, as the largest department of the US government, has access to more resources in general than other Interagency partners. During this period, ISAF maintained little to no relationship with MCIT and USFOR-A was being created and it had no capability to perform such coordination. USCENTCOM, who managed both major conflicts in geographically separated areas (Iraq and Afghanistan), was focused on Iraq. Personnel that worked at ASD/NII and NDU maintained relationships with personnel at MCIT and helped establish relationships between CJTF-101 CJ6 personnel and MCIT. Finally, the US Embassy did not replace the STA position, which left no one else to conduct coordination with MCIT personnel. CJTF-101 CJ6 personnel established a relationship with MCIT personnel in order to improve coordination for the ICT sector in Afghanistan, and it was the right decision.

The answer to the question, why was the CJTF-101 CJ6 (US Military) the lead planner/integrator of national ICT sector development in Afghanistan in 2008-2009, has

many answers and the simplest one is probably the best . . . because no one else was able to conduct this mission.

<div align="center">ICT as an Essential Service.</div>

Considering if ICT should be designated as an essential service, it is necessary to identify what services are currently identified as essential, in which documents and by what organizations, and the reasons why they are considered essential.

DoD doctrine defines essential services as the services required to sustain life and identifies these essential needs as availability of food, law enforcement, emergency services, water, electricity, shelter, health care, schools, transportation, and sanitation (trash and sewage).[4] DoS defines essential services as "security, the rule of law, economic governance, and basic human needs. . ." and provides integration of these services under its stabilization and reconstruction guidelines.[5] US Army doctrine provides examples of essential services (see Figure 3) and includes police and fire, water, electricity, schools, transportation work, medical, and sanitation (trash and sewage).

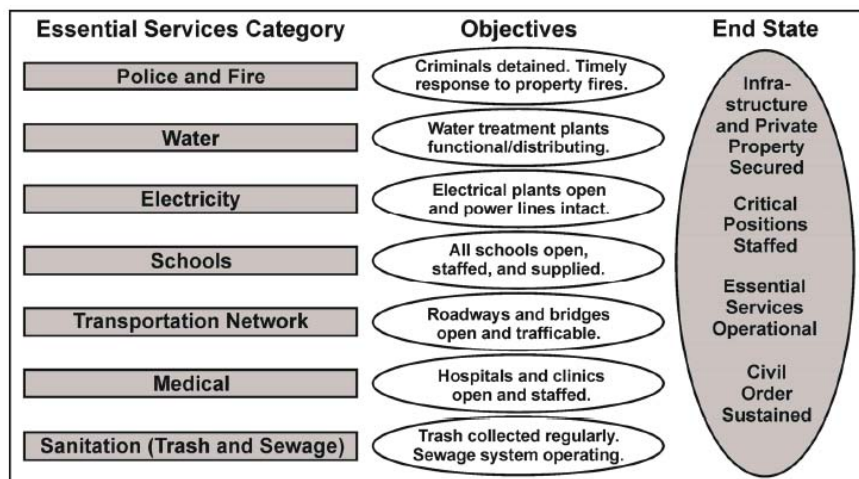| Essential Services Category | Objectives | End State |
| --- | --- | --- |
| Police and Fire | Criminals detained. Timely response to property fires. | Infra-structure and Private Property Secured |
| Water | Water treatment plants functional/distributing. | |
| Electricity | Electrical plants open and power lines intact. | Critical Positions Staffed |
| Schools | All schools open, staffed, and supplied. | |
| Transportation Network | Roadways and bridges open and trafficable. | Essential Services Operational |
| Medical | Hospitals and clinics open and staffed. | Civil Order Sustained |
| Sanitation (Trash and Sewage) | Trash collected regularly. Sewage system operating. | |

Figure 3.   Essential Services, Categories, Objectives, and End State
*Source:* Headquarters, Department of the Army, Field Manual (FM) 3-24, *Counterinsurgency* (Washington, DC: Government Printing Office, 2009), 5-15.

Due to the lack of a common definition of essential services, a cross-section of

essential services (see table 2) identified in multiple documents highlights a theory of

human needs developed by Albert Maslow, "Maslow's Hierarchy of Needs." Maslow

describes basic needs as "physiological, safety, love, esteem, and self-actualization" and

postulates that a human being will seek to satisfy these needs in a hierarchical order

beginning with satisfying physiological needs, then proceeding in sequence to the

remaining needs.[6] As it relates to the provision of services that are essential, it may be

that most humans follow a similar pattern. These needs are similarly identified in

governmental documents and identified as essential services.

Table 2.    Cross-Walk of Essential Services

| Maslow's Hierarchy of Needs | Essential Service (Consolidated) | DoD Definitions | DoS Definitions | Dept. of Army Definitions |
|---|---|---|---|---|
| Physiological | Basic Human Needs | - | Basic Human Needs | - |
| Physiological | Food | Availability of Food | - | - |
| Physiological | Water | Water | - | Water |
| Physiological | Shelter | Shelter | - | - |
| Physiological | Medical | Health Care | - | Medical |
| Physiological | Sanitation | Sanitation | - | Sanitation |
| Safety | Security | Emergency Services | Security | Police & Fire |
| Safety | Law Enforcement | Law Enforcement | - | - |
| Safety | Rule of Law | - | Rule of Law | - |
| | Economic Governance | - | Economic Governance | - |
| | Electricity | Electricity | - | Electricity |
| | Schools | Schools | - | Schools |
| | Transportation | Transportation | - | Transportation |
| Love | - | - | - | - |
| Esteem | - | - | - | - |
| Self-Actualization | - | - | - | - |

*Source:* Created by author.

On further analysis of this cross-section of essential services, it is evident that US

doctrine focuses on the physiological and safety needs identified by Maslow. However, it

is also evident there are several services that do not directly correlate to a basic human need. Specifically electricity, schools, and transportation are three services classified in doctrine as essential and are not clearly related to an essential human need. Each service, in a relative way, does influence the level to which other essential human needs are satisfied. For example, electricity can provide increased security by using electrical devices such as security alarms, lights, and electrical fences. Schools develop a higher level of education that can increase a human's capacity for self-preservation. Education can also increase the production of food and water. Additionally, schools educate humans to provide better medical care and sanitation. Transportation services improve distribution of food and water. It also allows improved security and increased medical care capabilities.

The ability for a service to improve multiple essential human needs could be identified as a cross-sector enabling service. Based on this same analogy, ICT services could also be considered a cross-sector enabling service. The use of ICT services enables communications that improve the production of food and water. ICT provides access to educational material that can improve the construction of protective shelters such as buildings and houses. ICT can be used to coordinate transportation, medical services, and even security.

ICT goes well beyond the two essential human needs, physiological and security addressed by the majority of the essential services necessary. ICT can be used for economic development, rule of law, and even to improve love and esteem. Through creative uses of ICT services, humans interact with other humans that without these ICT services they would not normally interact. This interaction can increase their ability to

share loving relationships over great distances and even across cultural boundaries. The possession of technology is a great way to build esteem in a community, especially when others lack such technology. ICT may even be capable of allowing humans to reach self-actualization through improved education and global interaction.

ICT is very useful in developing situational understanding of an operational area. Because of the geographical penetration capability of ICT services, it can be extended into contested areas with relatively low investments. Additionally, an increase in ICT services can directly improve local economies by enabling communications service entrepreneurs and retailers. ICT is a quick-win for a government attempting to show rapid economic progress.

When a government begins to establish creditability, one source of internal funding could be fees and taxes on ICT services. Spectrum usage fees, taxes on sales, and services are some ways governments can realize the enormous economic capability of ICT services. By using income from ICT services to finance government, ICT can increase the governments' effectiveness and legitimacy.

However, one negative aspect of ICT is that the technology is dependent on electricity. Each component of an ICT system relies on electrically powered equipment. A source of clean, stable power is required for ICT operations. Additionally, some parts of ICT are based on radio frequency (RF) technology. This RF technology is dependent on unobstructed use of the radio frequency spectrum.

Based on this analysis of ICT as an essential service, the conclusion is a resounding yes. Yes, ICT should be considered an essential service. This conclusion, if and when accepted by the appropriate US governmental authorities, requires the doctrine

to be updated to include ICT as an essential service. It also requires a change in the mindset of leaders conducting full spectrum operations to provide a focus on ICT during all phases of operations.

<div style="text-align:center">

The Importance of ICT to a Government
and its Society

</div>

ICT can be a powerful enabler for development, governance, information activities, and security. ICT can also be used to improve access to basic physiological human needs such as food, water, shelter, medical services, and sanitation. With the increased capability of a networked (using ICT) police force, general security, and law enforcement can be much more effective. ICT provides policing forces the ability to coordinate actions, inform masses of people, and enable faster response of first-responders where required. ICT also helps to ensure that the government can enforce its rule of law through coordination, collaboration, and the ability to keep greater detailed records. As a sector, ICT assists the government in the execution of economic governance by enabling organized banking and customer services. ICT is an enormous consumer of electricity and helps to ensure its demand and consumption. In schools, ICT can be utilized to teach greater amounts of knowledge to students, and even become a field of study itself. Through the coordination of transportation services, goods and services can be safely exchanged creating a market society that greatly benefits the citizens and therefore the government.

For these reasons, it is clear that ICT can enable a government to increase its legitimacy and improve its population. Nevertheless, there are other reasons to consider ICT as a benefit for government and societies. ICT connects individuals, communities,

and societies with information beyond their geographic boundaries.[7] This connection, especially in developing countries, can be used to improve local community efforts such as health care. This interconnectivity also allows interaction with the host-nation government, where an agency can publish how to acquire governmental resources, thereby enabling an informed population to take advantage of such resources as international aid.

With increased knowledge and capability, usually esteem is acquired. With esteem, a pride in oneself and a connection to ones government is reinforced. Societies begin to build pride and collectively, begin to support their central government because it has provided such services.

Beyond knowledge, pride, and capabilities, societies can develop a sense of self-worth. This connection with the external world, the esteem in their community, the pride in their country, and the capabilities to extend their wants and desires throughout our globally connected society may indeed assist, what Maslow calls, self-actualization. As citizens begin to self-actualize, they begin to identify and develop their talents. The process that began with the introduction of ICT services developed over time to help evolve a society into productive, informed citizens that support their government and enjoy their life.

In Afghanistan, one way to identify the importance of ICT to the government and its society was to identify the center of gravity (COG) for the GIROA. Identifying the COG required a consideration of the strategic mission. For this vision, President Obama declared to the world that a goal in Afghanistan was "we must strengthen the capacity of Afghanistan's security forces and government so that they can take lead responsibility for

Afghanistan's future."[8] According to this analysis, the "friendly COG" for MCIT in

Afghanistan, was Information Dominance. Defined as the ability to utilize the cognitive

domain of information warfare and to provide positive effects throughout the operational

environment, information dominance provides the Afghan government the ability to

develop perceptions (both internally and internationally), enhance awareness, supports

belief systems, and enables decision makers at the highest level of government. The

development and utilization of the cognitive domains enables Afghan government

official's access to all of their elements of national power, including the military, to

accomplish this strategic goal.

This COG has numerous critical capabilities and of them collaboration is the most

important. With access to information that is reliable, rapid, and continuous, the ability

for the government to coordinate actions across their DIME capabilities is crucial to its

effectiveness. Another critical capability is 'shared situational awareness' where all

decision makers have access to the same information and can develop similar awareness

of situations throughout the operational environment. Additionally, the ability for each

agency, organization, and ministry to 'self-synchronize' allows preemptive and

coordinated actions to occur simultaneously. A final critical capability is the ability to

develop 'new processes' as ICT develops and the government grows more competent and

develops it own way of doing business. The ability to adapt quickly to changes such as a

newly elected official is critical to maintain momentum for the overall government in

Afghanistan.

Critical requirements that allow this COG to function include the technical

capability of the 'ICT infrastructure,' the 'human capital' to install, operate, and maintain

the ICT infrastructure, and the ability to "protect and defend the information." Another, the development of a 'Chief Information Officer' structure throughout the government, including each of the elements of national power charged with providing, installing, operating, maintaining, and protecting ICT capabilities and managing the information environment. One additional critical requirement that is often not directly associated with ICT is access to reliable electricity. Because all current ICT capabilities require electricity (grid provided, locally generated, or battery powered) to operate, access to clean, reliable, and constant electricity is a necessity.

An analysis of the critical vulnerabilities is important to identify where to focus efforts to ensure that this COG is protected. First, we turn to the physical domain that contains the physical ICT infrastructure. As previously identified, the physical infrastructure can be extorted, rendered incapable, or destroyed by insurgent forces or local thieves. Intercepting or interrupting information and communications capabilities along the transport route, such as a cellular or microwave tower or transmission cable, present the greatest vulnerability. Another vulnerability that could be intercepted or disrupted is the electricity to power the ICT equipment by either disrupting or denying access to sustainable sources. More difficult to deny or disrupt is the electromagnetic spectrum that allows ICT to function in the physical environment. Disruption or denial of the spectrum requires access to sophisticated equipment, materials, and knowledge that is not likely to occur in the contemporary operational environment. It is more likely that unintended interference from an uncoordinated use of the spectrum could affect ICT transmissions rather than insurgents. With the increasing cyber capabilities across the world, any developing institution must create and maintain strict information protection

capabilities and a culture of information assurance at every level. Cyber-security is an absolute critical vulnerability in the information environment and must be integrated at the basic individual level of access.

Lastly, the most important vulnerability is the human domain in which technicians, operators, and users of information are vulnerable. From kidnappings, murder, extortion, and criminal mischief, to level of education and literacy, all present significant risks to the information environment and its effectiveness. The result of all actions within the ICT Sector serve only to interface with the information environment and are achieved in the human dimension; the ability to affect people is the ultimate goal.

This COG analysis serves only to illustrate the complexity of the situation that the CJTF-101 CJ6 faced in attempting to accomplish its mission. Because President Obama's remarks came after this deployment ended, it is likely that some lessons have been learned and put into practice. Additionally, the lack of a clear approach at the strategic level left much room for interpretation at the theater strategic, operational, and tactical level. Accomplishing one goal of the new strategy to enable the Afghans "so that they can take lead responsibility for Afghanistan's future" requires a clear theater strategic and operational level analysis of what actions are required and what conditions need to be set so that we can accomplish the President's stated goal and redeploy our forces. As an enabler for governments and societies, ICT provides the ability for coordination and synchronized operations for the betterment of people.

ICT Coordination as an Integral Part
of US National Strategic Policy

The lack of a clearly identified leader in the development of ICT integration causes each agency and department to define its own terms, establish its own internal rules of engagement, and provides the agency the ability to choose to address or not address the integration of ICT in the execution of national policy. Leaders simply have an expectation that communications will always be available. The overwhelming success of communications units and personnel to enable a commander's almost continuous communications capability has degraded the understanding of how these services are provided and at what costs. In this age of network centric warfare, the network may be considered a weapon system, but commanders and leaders expect that communications will be available everywhere and at all times, without exception. Indeed global communications are possible with the vast array of space segment, terrestrial, and subterranean communications systems, but all of these systems rely on numerous sources of power, RF Spectrum, lack of significant changes in nature (solar activity, earth quakes, hurricanes, etc.), and personnel trained and equipped to install, operate, and maintain this equipment. This vast array of ICT relies on the coordination of all the stakeholders to ensure that communications can be delivered as desired and if they cannot, mitigations measures are implemented to reduce the impact. This coordination is the crux of the issue for the implementation of national policy. The lack of a unified coordinator for ICT still exists and no agency, department, or element of the US government has been identified as the lead agent for this issue.

President Obama and his administration identified the need for a single point of focus within the federal government for the coordination of ICT and appointed the

nation's first Federal Chief Information Officer, Mr. Vivek Kundra.[9] This appointment also gives weight to the ICT council on which the Federal CIO is a member. However, even with this appointment, the Federal CIO position and the ICT council lack the capability to implement actions to provide and protect our ICT international and national interests.

In recent months, DoD has made significant improvements to the overall structure of its organizations to address the specific issue of global ICT integration. As the largest department of the federal government, DoD has the capability, training, and equipment to provide the monitoring, protection, and defense of our global ICT assets, also known as the global information grid (GIG). Under US Strategic Command, a new Joint Force Command has been established, Joint Task Force - Global Network Operations (JTF-GNO). The mission of JTF-GNO is to direct the operation and defense of the GIG as to assure timely and secure network centric capabilities for DoD strategic, operational, and tactical missions.[10] While the US pursues its national interest, the integration of policy, strategy, and capability resides at the GCC level under DoD. The GCC maintains the TSC plans and a standing Joint Interagency Task Force. Additionally, the GCC reports directly to the National Command Authority allowing direct access to decision makers at the highest levels of national power.

Due to the level of information collected, analyzed, and processed at the GCC level, and its ability to integrate with the other elements of national power to execute national strategy, it seems logical that DoD is the appropriate agency to coordinate and implement national strategic ICT policy. DoD is equipping and is reorganizing to meet this need. One shortfall is the training required to conduct national-level integration of

ICT with a host-nation. This training should include such courses as the Joint Command Control, Communications, and Intelligence course taught by Joint Forces Command.[11] Additionally, the lead integrator requires an element to conduct the daily business of such a task that could not be given to the already overburdened CCJ6. That element should include joint service and interagency personnel that have ready access to their primary agency. Additionally, ICT professional consultants could be utilized to ensure a cross-section of a civil-military approach. One such group was assembled in Iraq and was called the Iraqi Communications Coordination Group (ICCE).

Any such group or task force would require the direct participation of a US flag officer and a senior level executive from DoS, possibly the US Embassy, and the integration of any multinational stakeholders. It was obvious that the USCENTCOM Communications Officer (CCJ6) was engaged in the development of communications capabilities throughout the AOR but he did not have a specific staff element that could provide the DoD focus to be the lead department. An additional permanent staff element focused on integrating ICT throughout the entire AOR would enable the GCC better integration into the host-nation ICT infrastructure and could deploy on short-notice to provide the direct interface to the host nation government. Integration at this level would allow DoD visibility and the ability to integrate commercial solutions into plans and procedures for future commercialization of tactical communications networks.

USCENTCOM pioneered this effort in Iraq with the establishment of the ICCE. By making this an official function, assigned to a primary staff proponent, and maintaining visibility at the flag officer level, a greater amount of coordination could be achieved. As this element would be a permanent part of the GCC, it could serve as

continuity between the host-nation, such as Afghanistan, and the rotating CJTF's or ISAF elements. Officially tasking DoD with this responsibility, it would require a greater level of interaction among the interagency and the ability to address ICT issues and concerns during all phases of an operation. Greater amounts of training would be required for all personnel assigned to this task. This element would require resourcing and access to great amounts of information throughout the interagency. It would also require buy-in from the GCC commander to integrate this element into his staff. According to this analysis, DoD is clearly the best choice to be the lead integrator of ICT services in the execution of US national and international policy.

Specifically within DoD, USSTRATCOM, already tasked to provide and protect the GIG, is the best organization to conduct the ICT integration across the US Government. Due to USSTRATCOM's global area of responsibility and its existing relationship to other Interagency partners, the ability conduct coordination at the national strategic already exists. To complete the integration throughout other departments and organizations of the federal government, the Federal CIO needs the capability and authority to integrate policies with each CIO, such as the DoD CIO, in order to facilitate ICT integration throughout the government. DoD CIO already has a construct established to enable this coordination at the national and theater strategic levels through its cooperation with the Joint Staff J6.

The US Army has tasked Network Enterprise Technology Command (NETCOM) with executing the Army portion of the Global Information Grid, LandWarNet. The Global Network Enterprise Construct (GNEC) formally assigns responsibility to the Theater Signal Commands for executing the LandWarNet mission within each

Geographical Combatant Command AOR. With each GCC assigned a Theater Strategic Signal Command, the GCC is already equipped for the ICT coordination mission.

With the resources that DoD possesses and the missions already assigned to a structured enterprise, it is clear that DoD, through USSTRATCOM is the best choice to lead the ICT coordination efforts for full spectrum operations. Additionally, with a combined effort, such as a Forward Deployed Communications Coordination Element established within the AOR, even greater progress in ICT Sector synchronization could be achieved.

### The Integration of ICT in Full Spectrum Operations.

Examining the integration of ICT using the levels of war was useful due to the operational construct of our military operations. Current military strategy clearly defines the levels of war as strategic, operational, and tactical in which all full spectrum operations occur.

Beginning at the national strategic level, a review of national strategic documents did not reveal how the US government intended to integrate its elements of national power. No direction was provided to conduct an integrated, multifaceted, coordinated approach to our strategic problems. The current *National Security Strategy* was last updated in 2006.[12] Many significant changes occurred in the national strategic environment between 2006 and 2008 when 101st Airborne Division deployed to assume its wartime operational role as CJTF-101. According to Moore's Law, the technology doubled between the release of the national strategies and our engagement in Afghanistan.[13] As such, National Security Strategy direction was out of date with the technology that CJTF-101 would implement in during its tour.

During training for the deployment, the national focus remained on Iraq and Operation Iraqi Freedom. By all accounts, the operation in Afghanistan, Operation Enduring Freedom, was an "economy of force" mission.[14] According to 101st Airborne Division, the hierarchy of guidance followed national strategic, theater strategic, operational, and tactical correlations.[15]

National Strategic.

At the national strategic level, the US National Security Strategy (2006) did not establish any direction for the integration of ICT services.[16] Additionally, because the strategy was not updated, changes in technology greatly enhanced the network centric capabilities of the US government. Likewise, the US National Defense Strategy (2005) did not direct or addresses the integration of ICT.[17] Furthermore, the National Military Strategy (2005), correlated with the International Community (United Nations) Afghanistan Compact (2006), and the GIROA Interim Afghan National Development Strategy (2006) did not address ICT as a means or as a capability.[18] Unfortunately, in 2008 there existed no strategic guidance for the integration of ICT services or capabilities. At the national strategic level, it is imperative to integrate the ICT sector in order to establish, maintain, and/or protect critical communications infrastructure that enable governments to interact globally.

Theater Strategic.

The United Nations Security Resolution (UNSCR) designated Afghanistan a threat to international security that significantly threatened the nations of the North Atlantic Treaty Organization (NATO). The Supreme Allied Commander Europe

(SACEUR), Commander of NATO forces designated operations in Afghanistan a Non-Article 5 mission and assumed the lead international authority to execute the UNSCR directives. The United States retained its national caveat, as a country directly attacked, to execute Operation Enduring Freedom. USCENTCOM Theater Strategy (2006) and USCENTCOM Theater Campaign Plan (2007) provided the link between SACEUR's Operational Plan 1003 Rev1 (2005), Joint Forces Command Brunssum Operational Plan 30302 Rev 1 (2006). Additionally, the US Embassy in Kabul produced its Mission Performance Plan (2008). Between the theater strategic and operational level of operations, Combined Forces Command – Afghanistan and the US Embassy Kabul produced the Strategic Directive (2006). Although these are classified documents, the structure alone provides an understanding of the operational environment and the levels of operational control in Afghanistan. Clearly, interaction with the Government of Afghanistan was a strategic mission that should have been coordinated at the JFC Brunssum/USCENTCOM/USEMB Kabul level. At the theater strategic level, ICT integration is critical to ensuring regional stability and control by enabling the coordination of governments with neighboring nation-states.

Operational.

At the operational level, ISAF served as the lead for all NATO operations in Afghanistan. However, the US did not designate one single organization to serve as the lead and split the operation into two (and sometime three) separate missions. First was the Combined Joint Task Force (CJTF) that executed all Title 10, US Code responsibilities and served as the National Command Element (NCE) and National Support Element (NSE) for all US forces in the Combined Joint Operational Area.[19]

Designated with the mission to train and support the Afghanistan National Security

Forces (ANSF), the Combined Security Transition Command-Afghanistan (CSTC-A)

executed the responsibilities under Title 22, US Code. Additional Other Government

Agencies (OGAs) operated at both operational and tactical levels throughout the CJOA.

Under this construct Commander, CJTF provided all command and support functions for

all US national forces in the CJOA. Also dual-hatted as the ISAF Commander, Regional

Command (East), the CJTF commander and staff was required to support missions

throughout the CJOA including coordination with the Pakistani military and in all other

ISAF Regional Commands.

In early 2009, due to the increase in operational forces and the establishment of

new bases throughout the CJOA, operational needs outgrew CJTF capabilities. Under

General McKiernan's direction, as the US Senior National Representative (US SNR), an

"informational" staff was designated to support the role of the US SNR and to assist in

the coordination and execution of ISAF/OEF missions throughout the CJOA. Initial

personnel and support requirements were developed by CJTF-101 and provided by

realignment of existing Joint Manning Documents and personnel selected from the CJTF-

101 staff. The initial party of this element was setup in a building converted from a gym.

All communications assets had to be installed and all communications equipment had to

be reallocated from other priorities to create this ad-hoc staff element.

Shortly after this staff element became functional, its mission grew exponentially.

With the new presidential administration promising more troops in Afghanistan, the

mission quickly grew into a national command requirement. United States Forces-

Afghanistan (USFOR-A) was approved for implementation and personnel requests, many

of them by-name-requests for the best and brightest, flowed from Afghanistan to bring USFOR-A to full operational capability. In order to support CJOA wide requirements, planners wrote a Joint Urgent Operational Needs Statement for a Signal Brigade to assume the role of Joint Network Control Center–Afghanistan (JNCC-A). In May 2009, 7th Signal Brigade was designated and began deployment into the CJOA to serve as the JNCC-A. This construct, initially created in Iraq, provided one single organization responsible to coordinate and synchronize communications requirements for all US forces under Title 10, and the entire requirement for ANSF development under Title 22. This new JNCC-A was established at Bagram Airbase. During this transition, the CJTF-101 CJ6 staff served as the conduit for all interaction with MCIT. This was largely due to the personalities of the individuals and the personal connections with individuals at the Office of Assistant Secretary of Defense/Network Information Integrations branch. No record of the ISAF J6 meeting with MCIT personnel prior to this point could be found. However, it was noted that the ISAF Joint Spectrum Manager did meet with the Afghan Telecom Regulatory Authority (ATRA) and attended some of the Frequency Management Boards.

USCENTCOM J6's visible role in Afghanistan was evident upon the arrival of the USCENTCOM J6 and his direct interaction with COMISAF and the MCIT. Prior to this point, no Annex K (Command, Control, and Communications System) existed for the USCENTCOM Theater Campaign Plan. Shortly after the arrival of the J6, a communications planner was deployed to Bagram and collocated with the CJTF-101 CJ6. While deployed, the communications planner wrote Annex K for the campaign plan, while planning the arrival and transition of 7th Signal Brigade as the JNCC-A.

Additionally, the USCENTCOM Deputy J6 was designated as the USFOR-A J6 and deployed to Kabul. Upon the arrival of the USFOR-A J6, the CJTF-101 staff began transitioning designated CJOA-wide responsibilities to USFOR-A J6 and his limited staff. One of these tasks was the coordination and synchronization of ICT Sector development at the national level. By assuming this responsibility, USFOR-A became the lead-agent for meeting and synchronizing efforts with MCIT. However, due to the enormous responsibility of this new position and with a very limited staff, much of the actual coordination with MCIT remained with CJTF-101.

During this same period, the Defense Information Systems Agency (DISA) conducted site surveys in Afghanistan to determine the capability to provide DISA level communications infrastructure that would directly improve access to the global information grid and limit the amount of separate connections throughout the CJOA. The initial team designated three potential sites for integration due to their concentration of communications and infrastructure capability and their designation as key operational base locations; Bagram, Kabul, and Kandahar. Additionally, DISA leadership directed a forward element be deployed to coordinate the preparation and integration of DISA communications circuits, host-nation ICT infrastructure, and tactical-level communications assets. This team, designated as the DISA Support Element-Afghanistan (DSE-A), initially was a three-man team that established its headquarters in Kabul.

Throughout the CJTF-101 deployment to Afghanistan, significant debate continued as to who would be the lead-agent responsible for providing communications to the CJOA and for coordinating efforts with MCIT. As the communications operator, maintainer, and protector of operational base communications services for enduring bases

in support of USCENTCOM forces in Afghanistan, 25th Signal Battalion provided the infrastructure and support for major bases in Afghanistan.[20] As the theater communications integrator (COMMS-I), 335th Theater Signal Command (TSC) was directly responsible for the integration of all military and commercial communications in the USCENTCOM AOR.

During full spectrum operations, offensive, defensive, and stability actions are conducted simultaneously in some areas, and asymmetric in others. One offensive operation conducted by CJTF-101 was the attack on the information environment. In this instance, an attack that produced a significant way the operational force was sharing information. This change developed a favorable information environment that allowed Afghanistan to register its voters for the upcoming national election and conduct a multitude of other operations successfully. One such significant change was the integration and deployment of the Command Post of the Future (CPoF) system that promised a common operational picture (COP) for commander at all levels of the operational environment. This new system required significant changes to the operational environment of headquarters elements. Commanders and staffs at all levels required training in order to use this tool effectively. In addition, this system required significant bandwidth for effective operation. New network technologies were required to ensure this system could enable the commander and not hinder his execution of battle command. One significant restraint of this system was that it operated exclusively on US SIPRNET. In the combined, joint, interagency, and international environment, this proved a significant problem. The lack of information sharing proved to be a challenge for all headquarters. At coalition Brigade Combat Team (BCT) level headquarters, liaison

elements were required to provide access for the coalition brigade commander in order to update and receive guidance from the CJTF Commander.[21]

Defensive operations included actions such as co-locating towers on Forward Operating Bases (FOBs) where they could be protected by Soldiers. This was particularly useful when villagers were reluctant to take the first step in building a relationship with the ISAF Soldiers. In other locations, personnel from the village were hired as local security to protect the communications infrastructure. This provided a vested interest in the protection of the ICT equipment and jobs for the locals with little to no technical skills. In areas with a more educated population, not only were private security forces hired to protect the ICT infrastructure but local entrepreneurs could establish businesses by using the ICT services for profit, such as call centers, prepaid card dealers, etc.

As a stability mission, and due to the increased demand in bandwidth and a significant increase in locations to deliver communications access, CJTF-101 began researching the capabilities of the Afghanistan ICT infrastructure in order to provide, reliable, redundant communications throughout the AO. One such initiative, started by 82nd Airborne Division as CJTF-82 just prior to CJTF-101 arrival, was the use of terrestrial microwave links. During CJTF-101's deployment, engineers developed the network in a way that allowed a load-balancing effect across microwave links and the tactical network. One such company contracted in Afghanistan was the Afghan Wireless Communications Company (AWCC). On numerous occasions, planners and engineers met with AWCC personnel, toured their facilities, and developed mutually agreed procedures to improve network access. This was the first step to beginning the commercialization efforts in Afghanistan. Network access points were established at

remote locations such as FOBs and Company Outposts and transmitted along the microwave backbone to a central distribution hub.[22]

Another such stability operation designed to improve the development of Afghanistan was the contracting of Afghan Telecom to install an optical fiber cable link between Bagram and Kabul. The fiber cable was designed to be the initial step for Afghan Telecom to actually contract leased bandwidth across their optical fiber cable network. Additionally, ISAF and US militaries could greatly benefit from reducing their reliance on satellites and begin using such state-of-the-art capabilities in Afghanistan. As this initiative grew in popularity, more and more parties were interested in this capability. Almost overnight, the demand for high capacity, low latency transmission paths became the ultimate goal of several organizations. Unfortunately, this increased demand began to price local vendors out of the market. This level of competition ensured that only mega-organizations such as the US government could afford services. Once negotiations began on actually leasing the bandwidth, some provisions were put into place. As this project was originally designed to increase MCIT's capability to provide technical solutions to the significant logistical and technical problems of the link, to provide a source of revenue for MCIT, and to allow the contracting of services to private communications companies, these provisions limited the military's liability as the sole vender for MCIT. As long as the link was being used, private communications companies had priority to lease bandwidth capacity. As recently as July 2009, one such private communications company, Roshan, signed a three-year, multi-million dollar revenue producing lease from MCIT for bandwidth.[23]

The ISAF communications solution involved contracting communications support through a private communications company, Thales. This private company installed, operated, and maintained the ISAF Network through a series of satellite-based access points at various locations.[24] This network was called Full Operational Capability, Plus (FOC+) and provided users network access for computers, printers, scanners, etc while maintaining a communications helpdesk and hub in Kabul. ISAF J6 directed each of the Regional Commands in Afghanistan to support the FOC+ program. This program was run completely by civilians on contract with ISAF. This proved problematic in that the expansion capability was limited to existing locations. Additionally, simple network administration could not be conducted at the local level. For example, to allow one computer workstation to print to a local printer required a helpdesk trouble ticket that may sit in a queue for days before it was resolved. The lack of expansion capability caused many problems during the buildup of forces in Afghanistan during 2008-2009. New bases were established which were not covered by the existing contract. Because the bases required access to information systems and services, each Regional Command was required to supplement the base with their own national-based communications systems. This created an explosion of communications that could not pass information between them due to the national classifications of the systems and networks. These ISAF FOC+ systems were a semi-permanent installation, which means they could not be easily relocated. Due to the classification of these systems, the host-nation government was not allowed access to the ISAF networks. This made secure communications with the Afghan Government impossible. However, close coordination was still required to ensure operational level planning and integration could be accomplished. Most of this

coordination was conducted through unclassified email exchange, the internet, and face-to-face meetings.

Tactical

At the tactical level, Brigade Commanders contracted with local communications providers to install fiber-optic cables on their FOBs. This greatly reduced the need for tactical communications on the larger FOBs and allowed the commander to push his tactical assets down to the Battalion and Company levels. Additionally, Brigade S6s contracted microwave line of site transmission paths that reduced their reliance on SATCOM assets. Communications personnel met with local leaders to discuss their use and provided a conduit for the Afghan community leaders to request communications services. One such request was for a village in eastern Afghanistan, Chamkani, to receive communications coverage.[25] This request was processed through all available channels where it eventually received the attention of the Minister, MCIT. HE Sangin took personal interest to ensure the villagers received telecommunications services as requested. At the tactical level, military and civilian forces relied on the ICT infrastructure such as cellular telephone access for the majority of the communications needs. Additionally, tactical radios were used by military, police, and emergency first-responders to communicate. In some areas, portable radio stations were used to provide the public access to information from the government while military and civilian organizations handed out battery and hand-cranked powered radios to the Afghan people. By providing these ICT tools, the government quickly established legitimacy.

Summary

ICT should be integrated in full spectrum operations through unified action (UA).

Previously defined as the synchronization, coordination, and or/integration of the

activities of governmental and nongovernmental entities with military operations to

achieve unity of effort, UA is the overarching construct that provides coordination among

the Interagency.[26] UA involves the application of all instruments of national power,

including actions of other government agencies and multinational military and

nonmilitary organizations. In Afghanistan, unified action was lacking at all levels:

strategic, operational, and tactical.

As the operational level military headquarters in Afghanistan during 2008-2009,

CJTF-101 identified a lack of coordination in the ICT sector at all levels. The CJTF-101

CJ6 staff developed relationships, established coordination methods, and directed

resources that supported an integrated method of conducting operations. Although, ICT

Sector development was not a specified task in any order or plan, that task specifically

had to be accomplished in Afghanistan.

As a cross-sector enabler, ICT was a vital part of each of the currently identified

essential services. The identification of ICT as an essential service would greatly improve

the operational environment by requiring military commanders and other interagency,

intergovernmental, and private organization, to coordinate the protection, development,

and usage of the ICT sector throughout all phases of operations. Critically important to

improving government services, ICT was central to linking the Afghan society to the

global community.ICT is essential to full spectrum operations.

ICT provided access for governmental agencies and departments to cordinate efforts. The GCN provided a direct line of communication between the national level government down to provincial level leaders. This critical coordination enabled a synchronized apporach to providing disaster relief, crisis response, and information dessimentation. The ICT sector also provided a significant and steady income through taxes and fees. Through increased participatiation by the Afghan gonvernmement, the Afgan people were better informed and their quality of life increased.

The US government recognized the importance of ICT and developed both national and international capabilities under a DoD framework. Through that framework, assured access and protection of global ICT services was coordinated by the JTF-GNO. Regionally, JTF-GNOs proponent for ICT integration in the USCENTCOM AOR was the USCENTCOM TNOSC. As the directed representative of USCENTCOM for communications integration, 335th TSC was organized, trained and equipped, and tasked with the responsibility to coordinate the ICT sector throughout the AOR. However, due to the lack of resources in Afghanistan, 335th TSC provided only LNOs to assist CJTF-101 CJ6 with this coordination responsibiility. With the integration of the JIACG, the USCENTCOM J6 can provide better direction to the TNOSC and 335th TSC elements for closer coordination with MCIT. Additionally, the integration of organizations such as an Joint NetOps Control Center - Afghanistan could provide this coordination within Afghanistan in close cooperation with ISAF, USFOR-A, DoS, and other Interagency, Intergovernmental, and private organizations operating withing the AOR. With this level of coordination resources, DoD served a critical role of communications integrator for the ICT sector in Afghanistan.

In order to succently integrate ICT into full spectrum operations, the CJTF-101 required a knowledge of the operational environment, identification of stakeholders, and a clear endstate for the commerlization of communications capabilities in Afghanistan. Arguably, the CJTF-101during their tour in 2008-2009, never had any of these elements in the ICT sector of Afghanistan. Numerous attempts to identify the ICT infrastructure failed due to a lack of information sharing and collection capability. No clear leader in the ICT sector emerged to provide leadership and directfon for coordination, although MCIT made remarkable steps to improve their capability. No clear endstate was provided to any civil-military agency or department for the transition of communications capability that would relieve tactical communications assets for reassignment. Although CJTF-101 achieved remarkable success in their mission, this overall lack of cooordination in these three critical areas likely prevented the significant progress that the integration of ICT into full spectrum operations could have accomplished.

---

[1]Department of the Army, FM 3-0, 3-1.

[2]Ministry of Communications and Information Technology, Synchronization Meeting, 4.

[3]General George Casey, "SITREP of the Army" (Lecture, Command and General Staff College, Fort Leavenworth, KS, 16 April 2010).

[4]Chairman, Joint Chiefs of Staff, JP 3-24, II-7.

[5]United States Institute of Peace, *Guiding Principles for Stabilization and Reconstruction,* 8-98.

[6]Albert H. Maslow, "A Theory of Human Motivation," Originally Published in *Psychological Review*, 50: 370-396 (1943), 18.

[7]Wentz, 4.

[8]President Barak Obama, Remarks by the President in Address to the Nation on the Way Forward in Afghanistan and Pakistan, West Point, NY, 1 December 2009, 1-9.

[9]The White House, "President Obama Names Vivek Kundra Chief Information Officer," *Press Release*, 5 March 2009, 1.

[10]US Strategic Command, "USSTRATCOM Command Brochure," (Final Draft), http://www.stratcom.mil/files/brochure.pdf (accessed 10 May 2010).

[11]Joint Forces Command, "Joint C4 Planner's Course" (Fort Gordon, GA: Joint Forces Command, 2009), 1-2.

[12]The White House, *The National Security Strategy of the United States of America* (Washington, DC: Government Printing Office, 2006), 1.

[13]Gordon E. Moore, "Moore's Law," http://www.intel.com/pressroom/kits/ bios/moore.htm (accessed 18 April 2010).

[14]Spencer Ackerman, "The End of an Economy of Force Missions in Afghanistan?" *The Washington Independent* (June 2009), 2.

[15]CJTF-101 Joint Planning Group, "Hierarchy of Guidance" (Presentation for all JPG planners, Fort Campbell, KY: 2008).

[16]The White House, *The National Security Strategy*.

[17]Department of Defense, *The National Defense Strategy of the United States of America* (Washington, DC: Government Printing Office, 2008).

[18]Chairman, Joint Chief Staff, *The National Military Strategy* (Washington, DC: Government Printing Office, 2007).

[19]The US House of Representatives, *United States Code*, Title 10.

[20]Department of the Army, 25th Signal Battalion, http://www.25sigbn.army.mil/ default.html (accessed 1 April 2010).

[21]Charles D. Smith, "CJTF-101 CJ6 Report Regarding Observations at Forward Operating Base Ghazni; the Polish Task Force," 2008.

[22]Afghan Wireless Communications Company (AWCC), Afghan Wireless Microwave Backbone (document presented to author by AWCC, 6 April 2009).

[23]Ministry of Communications and Information Technology, Press Release, 12 July 2009.

[24]Thales Group, "Focus on FOC+ Service Contract for ISAF Network," http://www.thalesgroup.com/Pages/Event.aspx?id=7023 (accessed 18 April 2010).

[25]Oliver Dziggel, Electronic correspondence with author, 1 January 2010).

[26]Department of the Army, FM 3-0, 1-11.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

During their deployment to Afghanistan in 2008-2009, CJTF-101 demonstrated a way to integrate ICT into full spectrum operations. This case study identifies the relationships established, the projects started and/or completed, and the overall increase in capabilities and legitimacy of the Afghan government to provide for its citizens. This case study also identified several underlying concerns and significant potential ways to integrate ICT into full spectrum operations.

Conclusions Based on the Case Study

In identifying the agencies and departments operating in Afghanistan in 2008-2009, CJTF-101 was clearly more capable of conducting planning and integration of the ICT sector than any other element. First, using the DIME construct was a useful way to organize the discoveries, which identified a potential change to the construct itself. In the diplomatic element, coordination at the highest levels of government was required, but not necessarily achieved in the depth that provided the necessary effect on ICT development. The lack of a DoS representative to integrate the ICT sector was a significant factor in the lack of coordination at the national level between civil and military forces in Afghanistan.

In addition, having a DoS representative directly involved in the ICT sector would have better enabled a coordinated interagency effort and collaboration by sharing critical information about their actions with the host nation. As described by MCIT itself, the

ICT sector was very profitable and provided an engine for change that significantly affected the country's economics. Better security was a requirement for the ICT sector to develop and that security was beginning to be provided by the country's military forces and enforcement. All of these efforts combined to provide a more informed, responsive, and reliable government for the people of Afghanistan thereby support US strategic national interests in the region.

Another observation was that ICT should be considered an essential service. This classification as an essential service would allow leaders to commit more resources toward such a critical service as ICT. With the level of influence on essential human needs, ICT can serve as a cross-sector enabler for each of the other essential services. Through improved medical and educational capabilities, improved production of food and clean water, human existence can be improved. Through the coordination capability provided by ICT, security and transportation services can greatly improve the quality of life for people. With the capability to provide information to its people, the ability to coordinate responses to natural disasters, strategic threats to its borders, and by providing a funding source to the government, ICT can greatly increase a government's legitimacy. Going far beyond what the current essential services can provide, ICT can even begin to satisfy the higher human needs such as self-actualization. ICT synchronization is clearly essential to providing greater levels of integration in full spectrum operations.

With a clearer understanding about how the US government is organized at the national strategic level, it was easier to understand how ICT was, and was not, integrated and at what levels it was first addressed. It is evident that the military element of national power can drive ICT requirements during full spectrum operations. Although this may be

the most appropriate allocation of national power considering the capability of assets the military brings to an operation, the military was clearly not the sole integrator of ICT at the national strategic, theater strategic, or operational levels, nor even the tactical level of operations.

As shown through this research, CJTF-101 served as the lead integrator of ICT. However, it also shows the lack of training, resources and equipment required to perform such a critical responsibility by itself. Clearly, the assistance of DoS was required, as was the integration of other Interagency partners. The lack of a designated lead agent prevented a coordinated interagency and multinational approach. Additionally, without this agent being identified, there was no element integrated into the planning, execution, and assessment of the operational environment. The GIROA showed improvement but it was not from a synchronized, coordinated approach that encompassed all of the stakeholders in the ICT sector in Afghanistan. The CJTF-101 staff did integrate ICT into its operations; however, this integration was limited to the operational and tactical levels. Due to the immense amount of military presence, it is clear that DoD should have been specifically tasked, organized, and equipped to perform ICT sector development and integration in Afghanistan. This mission should have been further designated to 335th TSC. Finally, a coordinated effort, specifically supported by DoS, could have enabled the coordination of ICT services in the execution of US national and international policy in Afghanistan.

Recommendations

Significant changes in the overall US ICT strategy should be considered along with an increased national and international focus on the integration of ICT into the

planning and executing of any operation anywhere in the world. At the national strategic

level, the focus must span the entire governmental framework. The global information

grid is not an Army centric asset. The grid itself relies on and requires interconnectivity

and interoperability globally. Additionally, it requires the complete integration of

Information Operations and Global Command and Control that spans all levels of the

national strategic, theater strategic, operational, tactical, and interpersonal levels.

USSTRATCOM is the designated defender of the Global Information Grid for

DoD. However, no national organization exists that integrates ICT strategies into

international operations. This should become a strategic role for USSTRATCOM.

At the Theater Strategic level, the Geographical Combat Commander (GCC) has

authority and responsibility to integrate the National Security Strategy into the Theater

Security Cooperation Plans. For this purpose, the GCC should integrate its JIACG

element and an element of the J6 for a clearer picture of the ICT sector in the theater

AOR. For network communications (DoD centric), the GCC is assigned a Theater Signal

Command (TSC). The benefit of aligning the TSC with the GCC is to ensure that

integration and interoperability is managed at the theater level. The problem is that each

of these TSCs operates differently without standards of service across the GIG. With the

newly developed mission of USSTRATCOM to manage cyberspace, the overall

integration and protection of the GIG is the mission Joint Task Force Global Network

Operations (JTF-GNO). In order to conduct this mission, a new strategy of Global

Network Enterprise Construct (GNEC) was developed.[1] This construct operationalized

the Army portion of the GIG thereby enabling commanders to utilize ICT services as a

tool for the conduct of full spectrum operations. Therefore, JTF–GNO should coordinate

and with the Theater Network Operations and Security Center (TNOSC), assigned to every GCC. Additionally, the TNOSC should be tasked with overseeing the integration of commercial ICT capabilities within its AOR.

This new strategy, GNEC, is still in its infancy and will require significant oversight in the near future. The requirement to integrate ICT at the national and theater strategic level is clearly identified and this thesis describes the effects when that strategy was not well defined or executed at the operational and tactical level. This strategy must be well defined and capable of being implemented into current operations, specifically in Afghanistan. Once an ICT strategy is developed, approved, and implemented in CENTCOM, the TSCP will be updated, Campaign Plans modified, and appropriate organizations established and operational significant improvement can be expected.

In order to integrate ICT into full spectrum operations there should be changes to the training requirement for key personnel, improved information sharing capabilities developed, and full collaboration capabilities implemented to achieve strategic and operational goals. It may also be prudent to designate a "Lead Agent" to synchronize the efforts of stakeholders in the ICT sector. This agent must be empowered to direct or coordinate efforts across the full spectrum of national and international stakeholders operating within the operational environment. Current organizational structures may need adjusting to develop the capability to coordinate stakeholders and actors throughout the operational environment. Some key action items to consider are identified using the US Army's DOTMLPF construct:

(D) Designate Cyberspace as an element of national power (C-DIME).

(D) Require a true Whole-of-Government Approach to ICT Sector Development.

(D) Establish Direct Coordination with Host Nation Primary ICT Actors.

(D) Update doctrine to include the integration of cyberspace.

(O) Require all Joint and Interagency partners to synchronize lines of effort.

(O) Use a combined Lessons Learned Database.

(O) Require integration of ICT in Planning and Operations at all levels.

(O) Develop a Concept and Action Plan to Commercialize the Networks.

(O) Plan to transition network access at the earliest opportunity.

(O) Redistribute and redeploy communications assets; maintain a tactical reserve.

(T) Require all joint C4 Planners to attend JC4I School.

(T) Designate Cyber (Signal) representative in all PME (ILE and War College).

(M) Develop and use information sharing between ISAF/USG and the host nation.

(L) Designate COCOM G6 as theater integrator of ICT Sector

(P) Require a Civilian Surge must include ICT advisor to MCIT.

(P) Establish Afghanistan Communications Coordination Element in Kabul.

(F) Establish facility(s) where deployed environments are duplicated.

All of these recommendations are directly related to information derived from this study. Many of the recommendations would require significant changes but may produce significant results. In the Author's opinion, ICT integration is worth the costs.

<u>Summary</u>

Overall, the integration of ICT into full spectrum operations was being accomplished in Afghanistan, but not at the levels required for a stable peace. Additional attention is required for the ICT sector to become a viable capability in full spectrum operations. Additional research is recommended to determine the best way to integrate

ICT at the national and theater strategic levels. Future studies may be required to determine personnel and training requirements, as well as the restructuring of specific organizations and/or the possibility of developing new organizations. The costs required to implement these new strategies may pale in comparison to the efficiencies gained from the full integration of ICT into the operational environment.

---

[1]Chief of Staff, Department of the Army Memorandum, "LandWarNet--Global Network Enterprise Construct Strategy Implementation," 2 March 2009.

# GLOSSARY

Commercialization. Tactical theater level communications element installing the initial communications infrastructure and transitioning that capability to a commercial provider.

Cyberspace. The global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Full Spectrum Operations. Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment.

ICT Sector. As a sector, ICT supports national capacity building, export market focus, and plays a critical role in reestablishing basic economic linkages by relieving communication bottlenecks from financial, governmental, and cultural information flows.
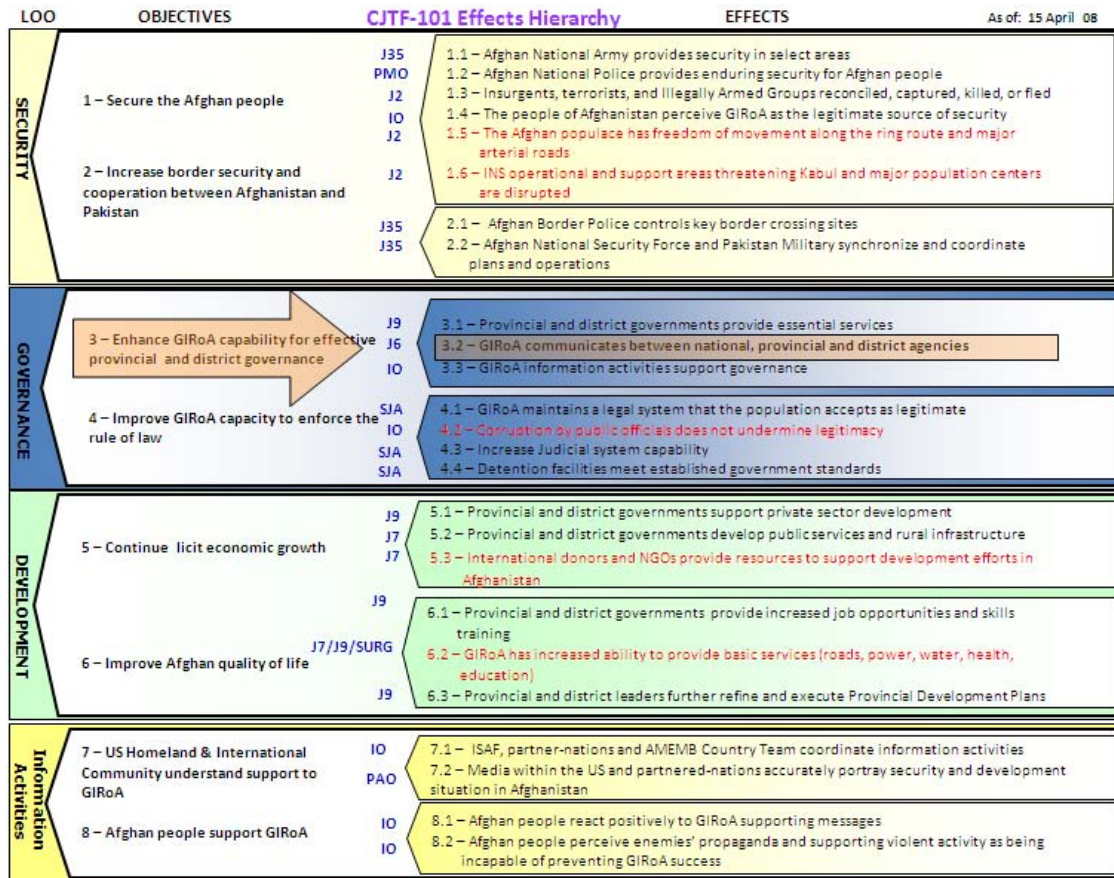
Interagency. United States government agencies and departments, including the Department of Defense.

Stability Operations. Stability operations are a subset of post-conflict operations. They are an overarching term encompassing various military missions, tasks, and activities conducted outside of the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.

# APPENDIX A

# CJTF-101 LINES OF OPERATION

This Lines of Operation (LOO) chart was used by CJTF-101 CJ6 in meetings with MCIT personnel and other stakeholders to help coordinate operations.



*Source*: Combined Joint Task Force (CJTF)-101 Staff, "CJTF-101 Campaign Plan" (Briefing by CJTF-101 staff at Joint Planning Group session, 6 March 2008).

BIBLIOGRAPHY


Books

Barnett, Thomas P.M., *The Pentagon's New Map: War and Peace in the Twenty-First Century*. New York, NY: G.P. Putnam's Sons, 2004.

Jorgensen, Danny L. *Participant Observation:A Methodology for Human Studies*. Newbury Park, CA: SAGE Publications, Inc., 1989.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations.* 7th ed. Revised by Wayne C. Booth, Gregory G. Colomb, Joseph M. Williams, and the University of Chicago Press Editorial Staff. Chicago, IL: University of Chicago Press: 2007.

US Institute of Peace, *Building Peace through Information and Communications Technologies*. Washington, DC: U.S. Institute of Peace, 2007.

World Bank Group. *Information and Communication Technologies A World Bank Group Strategy*. Washington, DC: The International Bank for Reconstruction and Development/The World Bank, 2002.

Yin, Robert K., *Case Study Research, Design and Methods.* Newbury Park, CA: SAGE Publications, Inc., 1989.

———. *Case Study Research: Design and Methods*. 4th ed. Thousand Oaks, CA: SAGE Publications Inc., 2009.


Periodicals

Armed Forces Communications and Electronics Association (AFCEA). *Signal Magazine* (March 2010): 1-89.

Global Alliance for ICT and Development (GAID). *Foundations of the Global Alliance for ICT and Development*. ed., Aliye P. Celik. New York, NY: United Nations, 2007.

Maslow, Albert H. "A Theory of Human Motivation." Originally Published in *Psychological Review*, 50: 370-396 (1943), 18.

Wentz, Larry, Frank Kramer, and Stuart Starr, Defense and Technology Paper 45, *Information and Communication Technologies for Reconstruction and Development: Afghanistan Challenges and Opportunities*. Washington, DC: Center for Technology and National Security Policy, National Defense University, 2008.

Government Documents

Chairman, Joint Chiefs of Staff. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, As Amended Through 19 August 2009. Washington, DC: Government Printing Office, 2009.

———. Joint Publication (JP) 3-0, *Joint Operations*. Washington, DC: Government Printing Office, 2006.

———. Joint Publication (JP) 3-13, *Information Operations*. Washington, DC: Government Printing Office, 2006.

———. Joint Publication (JP) 3-24, *Counterinsurgency Operations*. Washington, DC: Government Printing Office, 2009.

———. *The National Military Strategy*. Washington, DC: Government Printing Office, 2007.

———. "US Strategic Command Mission Statement." Offutt Air Force Base, NE: USSTRATCOM, 2009.

Department of the Army. *Army CIO/G-6 500 Day Plan: Delivering a Joint Net-Centric Information Enterprise*. Washington, DC: Government Printing Office, 2007.

———. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office, 2008.

———. Field Manual (FM) 6-0, *Mission Command: Command and Control of Army Forces*. Washington, DC: Government Printing Office, 2003.

———. Field Manuel Interim (FMI) 6-02.45, *Signal Support to Theater Operations*. Washington, DC: Government Printing Office, 2008.

Department of Defense. DoD Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*. Washington, DC: Government Printing Office, 2008.

———. *The National Defense Strategy of the United States of America*. Washington, DC: Government Printing Office, 2008.

Department of State. "FY 2009, Mission Strategic Plan. Kabul, Afghanistan: US Mission to Afghanistan." May 2007.

Islamic Republic of Afghanistan, Afghanistan National Development Strategy Secretariat. "Islamic Republic of Afghanistan; Afghanistan National Development Strategy-1387–1391 (2008–2013) A Strategy for Security, Governance,

Economic Growth & Poverty Reduction." Kabul, Afghanistan: Afghan Development Strategy Secretariat, 2008.

Maunder, Sanjoy. "Taleban Threat Hits Afghan Phones." *BBC News*. http://news.bbc.co.uk/2/hi/south_asia/7291833.stm (accessed 27 January 2009).

Ministry of Communications and Information Technology. "Islamic Republic of Afghanistan." http://www.mcit.gov.af (accessed 28 January 2009).

———. "Islamic Republic of Afghanistan ICT Sector Strategy (Draft)." 22 November 2007.

———. "MCIT (Afghan Telecom) and Roshan Sign MoU to Utilize OFC." Press Release, 12 July 2009.

———. Monthly Synchronization Meeting, MCIT Headquarters, Kabul Afghanistan, April 2008

———. "Summary of Achievements in the Year 1386." Brochure (April 2008).

United States Institute of Peace and the U.S. Army Peacekeeping and Stability Operations Institute. *Guiding Principles for Stabilization and Reconstruction.* Washington DC: United States Institute of Peace Press, 2009.

United States Strategic Command, "USSTRATCOM Command Brochure" http://www.stratcom.mil/files/brochure.pdf (accessed 10 April 2010).

White House, *The National Security Strategy of the United States of America.* Washington, DC: Government Printing Office, 2006.


Other Sources

Ackerman, Spencer. "The End of an Economy of Force Missions in Afghanistan." *The Washington Independent,* 2009.

Armed Forces Communications and Electronics Association (AFCEA). Website. http://www.afcea.org (accessed 27 September 2009).

Castelli, Christopher J. "Defense Department Adopts New Definition of Cyberspace." *Inside the Air Force*. http://integrator.hanscom.af.mil/2008/May/05292008/ 05292008-24.htm (accessed 20 March 2010).

Department of the Army. 25th Signal Battalion. http://www.25sigbn.army.mil/ default.html (accessed 1 April 2010)

Globalsecurity.org. 335th Theater Signal Command. http://www.globalsecurity.org/ military/agency/army/335tsc.htm (accessed 5 January 2010).

Harmonieweb. Applications. http://www.harmoneweb.org (accessed 30 December 2009).

International Telecommunications Union. "ICT Statistics Database." http://www.itu.int/ ITU-D/ICTEYE/Indicators/Indicators.aspx# (accessed 18 April 2010).

————. "The UN Millennium Development Goals." http://www.itu.int/ITU-D/ict/mdg/ (accessed 30 January 2010).

————. "World Summit on The Information Society Forum 2009." Brochure, May 2009.

Joint Forces Command. "Joint C4 Planner's Course." Fort Gordon, GA, 2009.

Moore, Gordon E. "Moore's Law." Intel Executive Biography. http://www.intel.com/pressroom/kits/bios/moore.htm (accessed 18 April 2010).

Thales Group. "Focus on FOC+ Service Contract for ISAF Network." http://www.thalesgroup.com/Pages/Event.aspx?id=7023 (accessed 18 April 2010).

The World Bank. *Information and Communications Technology-Glossary Guide.* 2009. http://go.worldbank.org/UPJ4PKMG60 (accessed 2 January 2010).

World Bank Group's Global ICT Department. *ICT and MDGs-A World Bank Group Perspective.* Washington, DC: World Bank Group's Global ICT Department, 2003.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Michael J. Burke
Department of Joint, Interagency, and Multinational Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Richard E. Berkebile
Department of Joint, Interagency, and Multinational Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Dr. John M. Curatola
Department of Military History
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301